IGEL Agent for Imprivata (IAFI) Configuration Guide

Microsoft AVD / Windows 365 Cloud PC RDSH/RDP Sessions

Version 1.0

February 2024

Based on:

UMS 12.3.0 and IGEL OS 11.09.150

Table of Contents

1.0: Introduction

IGEL has been an Imprivata technology partner for over a decade. This partnership has empowered thousands of healthcare users to achieve secure, quick, and easy access to virtualized clinical applications and desktops using IGEL OS-powered endpoints.

In 2022, we officially expanded the IGEL and Imprivata partnership to develop a new agent to deliver enhanced integrations and enable new workflows to address increasing market and customer demands.

2.0: Overview – IGEL Agent for Imprivata (IAFI)

IMPORTANT: IAFI is a free licensed feature with an initial set of supported workflows today and a roadmap of new features planned for later releases. As such, we require validation of supported workflows prior to providing the license(s) for customer testing or production.

The IGEL Agent for Imprivata (IAFI) is our implementation for various Imprivata OneSign related workflows. In contrast to Imprivata's ProveID Embedded (PIE) Agent which uses the IGEL Appliance Mode option (OS 11 only), the IGEL Agent for Imprivata (IAFI) was created as a "non-appliance mode" licensed feature which allows full access to the IGEL Desktop and the enablement of supported use cases.

In the default configuration, the Agent docks into the IGEL OS system tray (bottom right corner) and is controllable via a context menu. There is also a Full Screen Lock option with authentication tiles similar to what the PIE agent login screen looks like.

The IAFI is integrated into the IGEL OS 11 firmware and is also available as an IGEL OS 12 application from the IGEL App Portal. IAFI was built to focus on:

- A non-appliance mode experience providing IGEL OS local desktop access combined with application and desktop virtualization scenarios
- Support for Microsoft Azure Virtual Desktop (AVD) and Windows 365 integration and other desktop and application virtualization workflows (Citrix, VMWare, Fast User Switching)
- Device Location based override option policy to enhance Imprivata VDA user policy

The IGEL Agent for Imprivata (IAFI) is built and maintained by IGEL whereas in contrast, Imprivata builds and maintains their ProveID Embedded (PIE) agent. Like the Imprivata PIE agent, the IAFI utilizes the Imprivata ProveID Web API - a proprietary Imprivata protocol that encapsulates in TLS for secure communication with the Imprivata virtual appliances.

Customers have flexibility to use both agent options based on their requirements and supported workflows with either agent.

2.1: Overview- IGEL and Imprivata Agent Options

ProveID Embedded - PIE Agent	IGEL Agent for Imprivata (IAFI)
Built and Maintained by Imprivata	**Built and Maintained by IGEL**
IGEL Appliance Mode Only Experience • No IGEL local desktop access	Non-Appliance Mode Experience • Allows IGEL local desktop access
Uses ProveID Web API • Requires Imprivata VDA licensing • Imprivata and IGEL OS Version dependencies	Uses ProveID Web API • Requires Imprivata VDA licensing • Backward compatible to older Imprivata versions (7.6 or higher)
PIE Agent downloaded from Imprivata appliance and installed on IGEL OS 11 via bootloader	OS 11 agent built into firmware • Licensed Feature - Workspace Edition Add-on that enables the feature • Supported use case validation required
Supported workflows, use cases and roadmap developed by Imprivata	Supported workflows, use cases and roadmap developed by IGEL
Not supported on IGEL OS 12	OS 12 app available in the IGEL App Portal

2.2: IGEL Agent for Imprivata – Supported Features Overview

- See Appendix B for the entire feature matrix.

<table>
<tr><th colspan="2">IAFI General Feature Overview - as of IGEL OS 11.09.150</th></tr>
<tr><td>Logon Screen with Customization
• Compact Mode (default setting)
• Full Lock Screen
• Specify Default Domain

Primary Authentication Methods via Logon
• Password
• Password + Change PW (expired PW)
• Password + Change PW (New PW invalid)
• Proximity Card – no 2nd factor
• Proximity Card + PW
• Proximity Card + PIN
• Proximity Card + PIN (PIN not enrolled)
• Tap Proximity Card to Lock / Unlock
• Tap Over previous user
• Grace period for second authentication factor (PIN or Password)

Enrollment
• Password
• Proximity Cards / Number of cards allowed to enroll / Allow users to enroll replacement card
• Imprivata PIN / PIN Length / Expiration / Do Not Allow / Complex PIN
• Question & Answer</td><td>Automatic License Deployment for IAFI WE Add-On license

Multi-Monitor Support
• NOTE: monitors must be same resolution

Appliance Failover support
f
Reports Agent/OS version within Appliance

Non-OneSign User VDI access
• VDA computer policy feature

Imprivata Virtual Channel
• Microsoft RDP/AVD/Cloud PC, Citrix, VMWare
• Proximity Readers Only

Authentication Devices
• Imprivata rf IDEAS Readers

Logging Levels
• info, debug, critical</td></tr>
</table>

3.0: Imprivata System Requirements

3.1: OneSign Appliance Versions (on-prem or Azure deployed)

- G4 Appliances: 7.10 and higher
- G3 Appliances: 7.6-7.10
    - **IMPORTANT:** Imprivata no longer supports the G3 appliance or versions running on this platform. IAFI can still work with the ProveID Web API running on G3 appliance versions, but customers should migrate to the G4 appliances for production use.

3.2: Licensing

- **REQUIRED:**
    - Authentication Management (AM)
    - Single Sign-On (SSO)
        - IGEL OS 11.09.150 and any Private/Public Build based on this version.
    - Virtual Desktop Access (VDA)
    - ProveID Web API
- **OPTIONAL:**
    - Self Service Password Reset (SSPR)
        - NOTE: IAFI supports enrollment of Questions and Answers used for SSPR but will add support for Q & A login or SSPR in a future release.

3.3: Configure the OneSign Admin Console for ProveID Web API access

1. Open the OneSign Admin Console.
2. Log in as an administrator.
3. On the upper-right corner of the page, **click the gear icon**, and in the drop-down menu, click **API Access**.
4. In the **ProveID - API Access and Security** section, select the **Allow full API access via ProveID Web API and ProveID Embedded**.
    a. NOTE: Restricted API Access is not supported at this time.
5. Select the **IGEL OS** check box.
6. Save the configuration.

3.4: Deploy the Imprivata Appliance Certificate(s) to IGEL Devices

IGEL supports the Imprivata appliance cert(s) in either the Base64 encoded X.509 **.crt** or **.cer** format. By default, Imprivata Appliances use a Self-Signed certificate (**.crt** format) generated by the Imprivata Root CA that is built into the appliance.

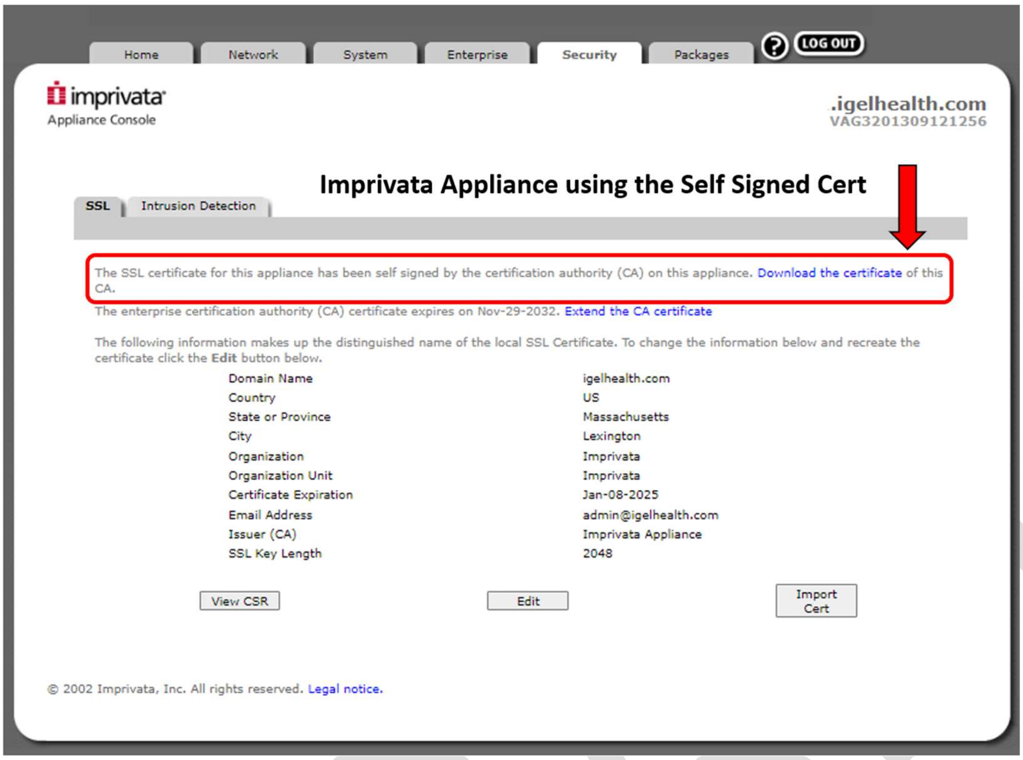
Customers can change the appliance certificate to one that is signed by a Trusted Root CA for either their network (ex: Active Directory Domain Enterprise Root CA) or a Publicly Trusted CA like DigiCert. If this is the situation, then you will need to export the Root CA / Subordinate CA / Appliance Cert chain in Base64 X.509 .crt or .cer format and deploy the chain to all to the devices via the UMS. See section 3.4.3

3.4.1: Using the Imprivata Root CA Certificate

To confirm a customer is using the Self Signed certificate, log into the Imprivata Appliance Console and go to the Security tab. (ex: Appliance URL is: **https://fqdn-of-appliance:81**)

You should see a message that says:

"The SSL certificate for this appliance has been self signed by the certification authority (CA) on this appliance. Download the certificate of this CA."



Imprivata Appliance using the Self Signed Cert

The SSL certificate for this appliance has been self signed by the certification authority (CA) on this appliance. Download the certificate of this CA.

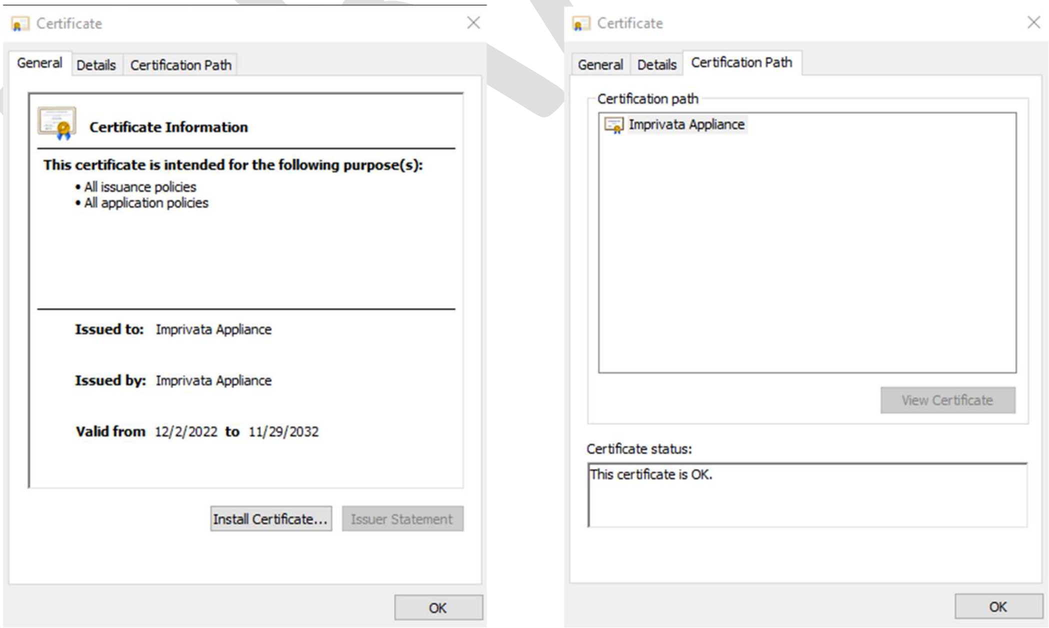
The enterprise certification authority (CA) certificate expires on Nov-29-2032. Extend the CA certificate

The following information makes up the distinguished name of the local SSL Certificate. To change the information below and recreate the certificate click the **Edit** button below.

Domain Name	igelhealth.com
Country	US
State or Province	Massachusetts
City	Lexington
Organization	Imprivata
Organization Unit	Imprivata
Certificate Expiration	Jan-08-2025
Email Address	admin@igelhealth.com
Issuer (CA)	Imprivata Appliance
SSL Key Length	2048

© 2002 Imprivata, Inc. All rights reserved. Legal notice.

1. Click the **Download the certificate** option.
2. This should automatically download the Root certificate as a file called: **ssoCA.crt**



Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

Issued to: Imprivata Appliance

Issued by: Imprivata Appliance

Valid from 12/2/2022 **to** 11/29/2032

Certification path

Imprivata Appliance

Certificate status:

This certificate is OK.

Properties of the Imprivata Root Certificate (ssoCA.crt)

The Imprivata Root CA certificate is the only one you need to deploy to the IGEL devices from the UMS Console as it will verify the trusted connection to the different appliances in the environment. **Proceed to section 3.4.3**

3.4.2: Using a Third-Party Root CA (ex: Microsoft AD or Public CA)

In this situation, you will not be able to download the Root CA from the Imprivata Appliance Console. You will have to export the chain via a browser supported by the Imprivata Appliance Console (MS Edge or Chrome).

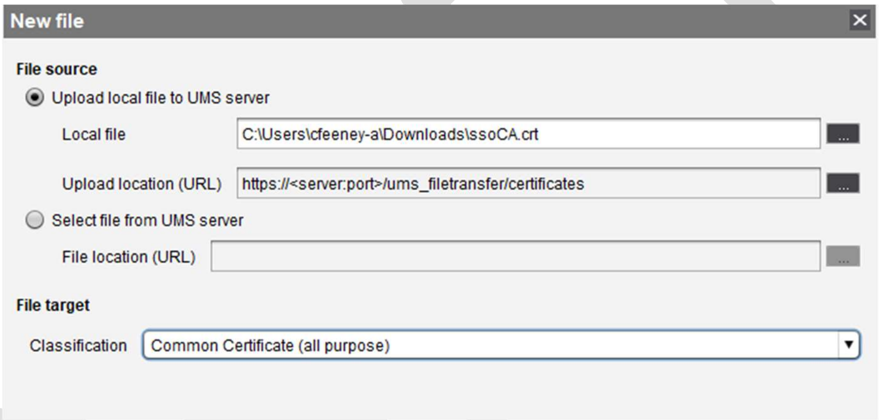
Export the certificate chain in .crt format (Base64 X.509). **Proceed to section 3.4.3**.

3.4.3: Deploying the Appliance Certificates

See this IGEL KB article for how to deploy certificates via the UMS Deploying Trusted Root Certificates in IGEL OS

When uploading the Imprivata Root CA certificate or Third-Party certificate(s) to UMS, you can choose either of two options for file classification:

- Common Certificate (all purpose) → **preferred choice**
- SSL Certificate



New file

File source

● Upload local file to UMS server

Local file: C:\Users\cfeeney-a\Downloads\ssoCA.crt

Upload location (URL): https://<server:port>/ums_filetransfer/certificates

○ Select file from UMS server

File location (URL):

File target

Classification: Common Certificate (all purpose)

Uploading Imprivata Appliance certificate into UMS as Common Certificate classification

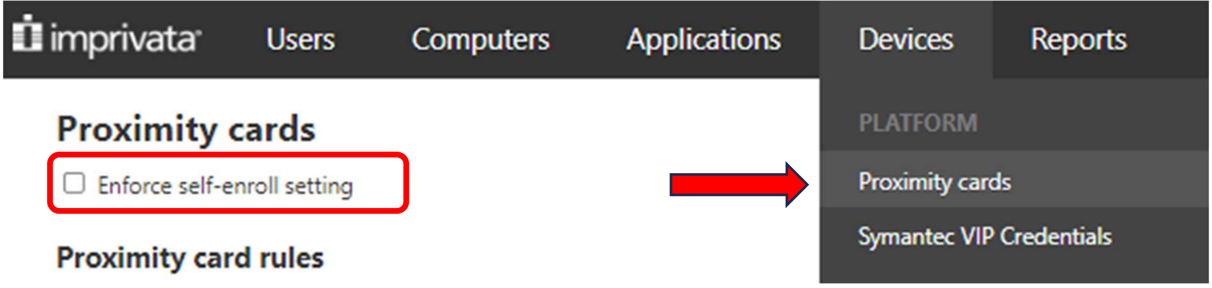
With either option, once the certificate is deployed to the device, it will automatically install in the **/wfs/ca-certs** directory which is where the IGEL Agent for Imprivata looks for the certificates. If needed, you can verify the certificate by opening a terminal window and running the following command:

cd /wfs/ca-certs; openssl verify ssoCA.crt or **cd /wfs/ca-certs; openssl verify ssoCA.cer**

3.5 Proximity Card Allow List- Self Enrollment

IMPORTANT: Do not enable this for IGEL Agent for Imprivata use.

1. In the Imprivata Admin Console, go to the Devices menu > **Proximity cards** page
2. Uncheck **Enforce self-enroll setting**.



Proximity cards

□ Enforce self-enroll setting

Proximity card rules

When you enable the proximity card "Allow list", you control what specific proximity cards users can self-enroll. See **Imprivata KB article 23313** for an explanation of this setting.

With this option selected, users can only self-enroll a proximity card when:

- The card is listed on the Proximity cards page, and
- the assignment status is set to **Available**, and
- a check mark appears in the column **Allow Self-enrollment**.

If a user attempts to enroll a proximity card that does not appear on the Allow list, then an error message appears.

3.6 – Imprivata Computer and User Policies

These will be covered in Section 7 Authentication Only Workflow and Section 8 Follow Imprivata Policies and Workflows.

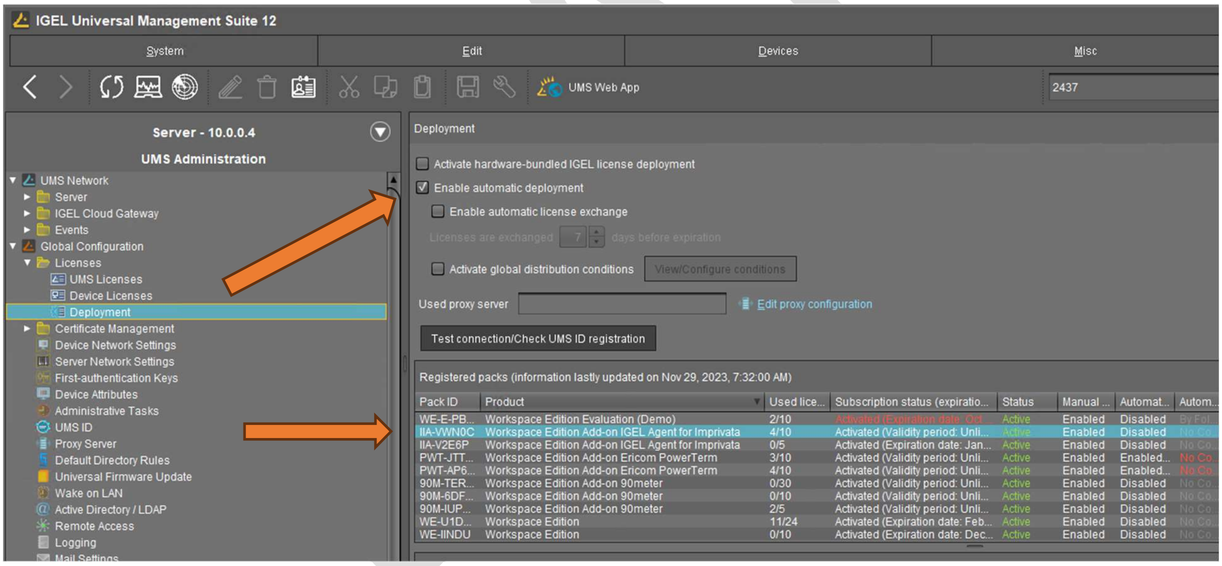
4.0: IGEL System Requirements

4.1: UMS

- 6.10.140 (minimum version)
  - For customers not upgraded to UMS 12, we recommend the UMS 6.10.150 private build
  - Contact IGEL Support for a download link
- 12.x or higher

4.2: Licensing

- Active subscription and maintenance of either:
  - Workspace Edition (WE) or COSMOS PAS
    - See this: IGEL COSMOS PAS - Entitlements and Effects of Expiration
- IGEL Agent for Imprivata Workspace Edition (WE) Add-On
  - Use case approval is required before providing any licenses for customer testing or production use. **See section 6.2 for approved use cases for Microsoft AVD/W365/RDSH/RDP**.
  - Request Form: IGEL Agent for Imprivata Request Form
  - IAFI licenses are provided as a **Delivery Token** that must be registered within the IGEL License Portal by the customer. Redeeming a Delivery Token (Legacy) (igel.com)
  - The EULA must be accepted and then the IAFI product pack will be available to assign to a UMS Server for Automatic License Deployment (ALD).



Deployment

☐ Activate hardware-bundled IGEL license deployment

☑ Enable automatic deployment

☐ Enable automatic license exchange

Licenses are exchanged 7 days before expiration

☐ Activate global distribution conditions View/Configure conditions

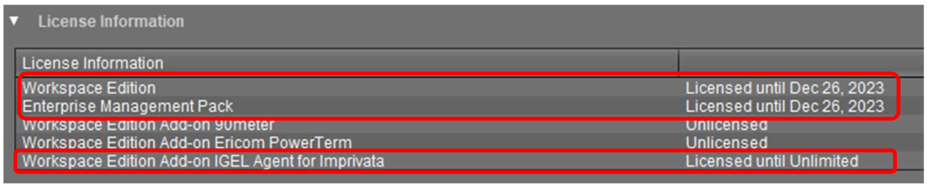
Used proxy server Edit proxy configuration

Test connection/Check UMS ID registration

Registered packs (information lastly updated on Nov 29, 2023, 7:32:00 AM)

Pack ID	Product	Used lice...	Subscription status (expiratio...	Status	Manual ...	Automat...	Autom...
WE-E-PB...	Workspace Edition Evaluation (Demo)	2/10	Activated (Expiration date: Oct ...	Active	Enabled	Disabled	By Fol...
IIA-VWN0C	Workspace Edition Add-on IGEL Agent for Imprivata	4/10	Activated (Validity period: Unli...	Active	Enabled	Disabled	No Co...
IIA-V2E6P	Workspace Edition Add-on IGEL Agent for Imprivata	0/5	Activated (Expiration date: Jan...	Active	Enabled	Disabled	No Co...
PWT-JTT...	Workspace Edition Add-on Ericom PowerTerm	3/10	Activated (Validity period: Unli...	Active	Enabled	Enabled...	No Co...
PWT-AP6...	Workspace Edition Add-on Ericom PowerTerm	4/10	Activated (Validity period: Unli...	Active	Enabled	Enabled...	No Co...
90M-TER...	Workspace Edition Add-on 90meter	0/30	Activated (Validity period: Unli...	Active	Enabled	Disabled	No Co...
90M-6DF...	Workspace Edition Add-on 90meter	0/10	Activated (Validity period: Unli...	Active	Enabled	Disabled	No Co...
90M-IUP...	Workspace Edition Add-on 90meter	2/5	Activated (Validity period: Unli...	Active	Enabled	Disabled	No Co...
WE-U1D...	Workspace Edition	11/24	Activated (Expiration date: Feb...	Active	Enabled	Disabled	No Co...
WE-IINDU	Workspace Edition	0/10	Activated (Expiration date: Dec...	Active	Enabled	Disabled	No Co...

UMS Server Licensing with IAFI WE Add-On enabled for automatic deployment



License Information	
Workspace Edition	Licensed until Dec 26, 2023
Enterprise Management Pack	Licensed until Dec 26, 2023
Workspace Edition Add-on 90meter	Unlicensed
Workspace Edition Add-on Ericom PowerTerm	Unlicensed
Workspace Edition Add-on IGEL Agent for Imprivata	Licensed until Unlimited

IGEL OS device with IAFI WE Add-On License installed

5.0: Microsoft Requirements

5.1: Licensing

The customer must already be licensed for one or more of these Microsoft virtual desktop offerings:

- AVD
- Windows 365 Cloud PC
- On-prem RDSH environment (ex: TS CALs)

PREREQUISITE: The customer must have these environments up and running and accessible from an IGEL OS endpoint via a manual login (i.e. Password Authentication) using the IGEL AVD / Windows 365 or RDP client.

5.2: Microsoft Entra Hybrid-Joined AVD or Windows 365 Cloud PC resources

REQUIRED: Entra Connect Sync with Password Hash configured - Because the Imprivata Enterprise Appliances are synching with the on-prem Active Directory domain, in order to access Azure Entra resources, the customers domain must be synching with their Azure Entra ID domain tenant via the Entra Connect Sync (formerly DirSync and Azure AD Sync).

- By default, the Microsoft Entra user Principal Name (UPN) is set to the same value as the on-premises Active Directory UPN.
- The Entra Connect Synchronization is bi-directional so that the UPN values match.
- The end user's email address is often an example of the UPN needed to access Microsoft Entra Azure resources like AVD or Cloud PC.

REQUIRED: Password Hash Synchronization keeps the Entra ID and on-prem Active Directory passwords in synch so a user can access resources in both environments. See this for more information.

PREREQUISITE: Confirm with the customer that the UPN values and email address match for both the on-prem Active Directory and Entra ID.

5.2.1: Verify the UPN and Email Address Match

IMPORTANT: Imprivata Appliance and Active Directory User Account synchronization

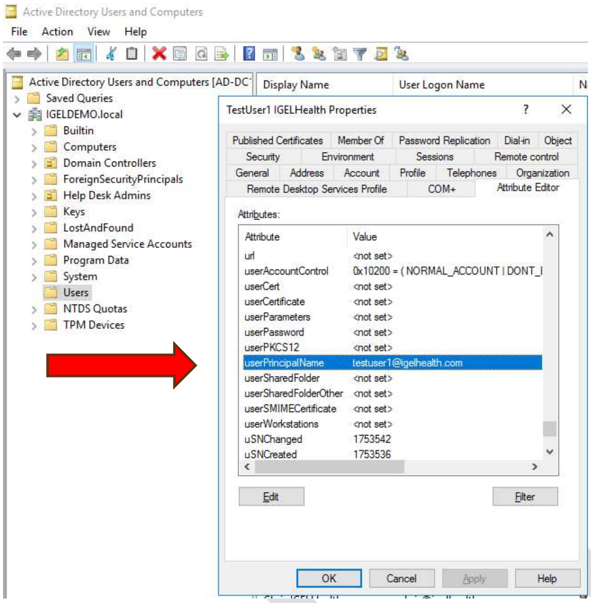
- The appliance can synch the email address and provide that information to our IGEL Agent for Imprivata via the Web API call we make during authentication. The user's email address imported into the Appliance, should match the UPN needed for accessing Entra ID / AVD resources.

In this example, the **Imprivata appliance** is synchronized with the local Active Directory which in turn, is synchronized with the Microsoft Entra ID Tenant via the Entra Connect Synch.

Local Active Directory Domain:	**igeldemo.local**
Microsoft Entra ID Tenant:	**igelhealth.com**
Entra ID UPN / Email address:	**username@igelhealth.com**

Verify the UPN in Active Directory

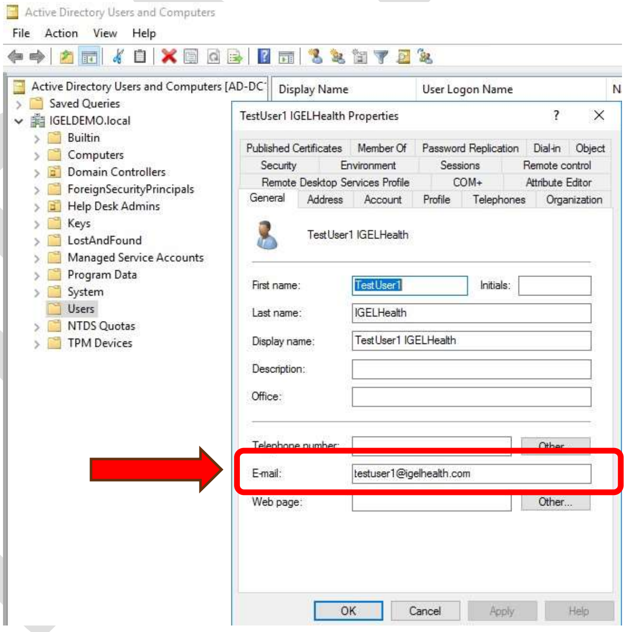
- Open **Active Directory Users and Computers MMC – View – Advanced Features**
- Open the **user properties** for someone that has entitlements to AVD
- Go to **Attribute Editor – userPrincipalName**
- The UPN value seen here needs to match the Entra ID UPN.



Attribute	Value
url	<not set>
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_I
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	testuser1@igelhealth.com
userSharedFolder	<not set>
userSharedFolderOther	<not set>
userSMIMECertificate	<not set>
userWorkstations	<not set>
uSNChanged	1753542
uSNCreated	1753536

Example UPN attribute is testuser1@igelhealth.com which is synchronized between Active Directory and Entra ID

Verify the email address in Active Directory matches the Entra ID UPN



First name: TestUser1 Initials:

Last name: IGELHealth

Display name: TestUser1 IGELHealth

Description:

Office:

Telephone number:

E-mail: testuser1@igelhealth.com

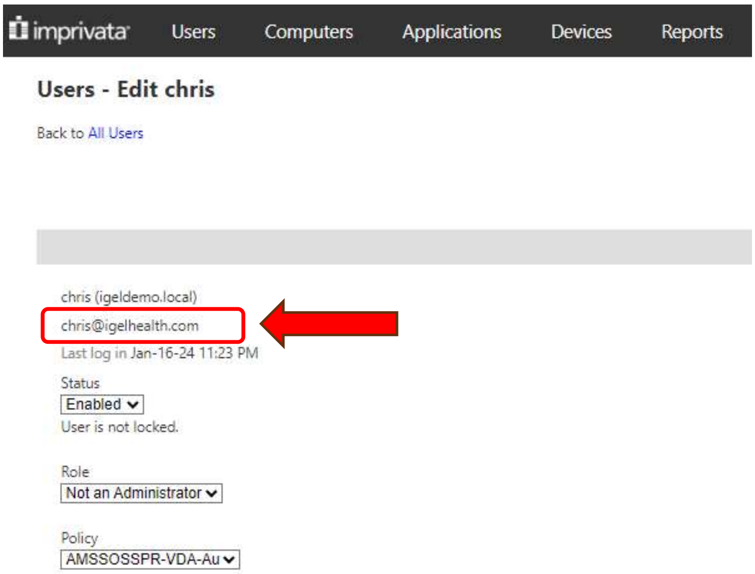
Web page:

Active Directory Users and Computers – User Properties – General Tab – Email

This should match the UPN value in Attribute Editor and will be imported into the Imprivata Appliance.

Verify the Imprivata User account has synched the email address from Active Directory

Log into the Imprivata Appliance and check a user account properties to confirm that the email address is imported and matches the Entra ID.



Users - Edit chris

Back to All Users

chris (igeldemo.local)

chris@igelhealth.com

Last log in Jan-16-24 11:23 PM

Status
Enabled

User is not locked.

Role
Not an Administrator

Policy
AMSSOSSPR-VDA-Au

Imprivata user account email address – same as Entra ID UPN

5.3: Imprivata Agent for the Hybrid Joined AVD or Windows 365 Cloud PC

To install the Imprivata Windows agent in the AVD or Cloud PC image, these resources must be Hybrid-Azure AD joined. This will allow the Imprivata Windows agent to go online when the user is authenticated to the AVD or Cloud PC resource.

- See this for more information: Hybrid identity documentation - Microsoft Entra ID | Microsoft Learn

Hybrid Joined devices must first successfully sign-in against the Active Directory (AD) domain. The Imprivata agent will use the AD domain account to go online. The users AD UPN is sent to Microsoft Entra ID. Given the required synchronization, the user should be logged in successfully to their AVD or Win 365 virtual desktop.

To satisfy this requirement, the IGEL Agent for Imprivata (IAFI) will:

- Authenticate against the Imprivata appliances using the on-prem AD domain user identity (either Password authentication or Badge Tap)
- Once authenticated, the appliance will return the email address and domain password which IAFI will use to start the AVD / Cloud PC client to access these resources. This requires the use of password hash synchronization with Microsoft Entra ID.

6.0: IGEL Agent for Imprivata (IAFI) Configuration Options

6.1: IAFI Workflow Descriptions

There are two main workflow options with IAFI: **Authentication Only** or **Follow Imprivata Policies and Workflows.**

Authentication Only	Follow Imprivata Policies and Workflows
Description	**Description**
• IAFI uses the Imprivata Appliance for Authentication, checks VDA licensing but does not use the Computer or User Policy VDA settings to initiate the workflow. • IAFI augments Imprivata VDA policies with additional workflow flexibility by using a preconfigured session. • IAFI securely inserts user credentials delivered from the Imprivata appliance into a local IGEL preconfigured session to drive the workflow. • This mode is **REQUIRED** for AVD/Cloud PC sessions but can also be used with Microsoft RDP preconfigured sessions.	• This is the default workflow setting for IAFI and requires a proper setup on the Imprivata appliance for VDA user and computer policies. • IAFI behaves like the PIE agent and will use the VDA User and Computer Policies when a user authenticates to automate the workflow • **Location Based Override**: one benefit is that unlike PIE, IAFI supports the ability to launch a preselected (named) resource for on-prem Citrix, VMWare Horizon or Microsoft RDP resources • In this mode, IAFI does not use a preconfigured session like the Auth Only mode.

6.2: IAFI Approved Workflows for Microsoft AVD / W365 / RDP

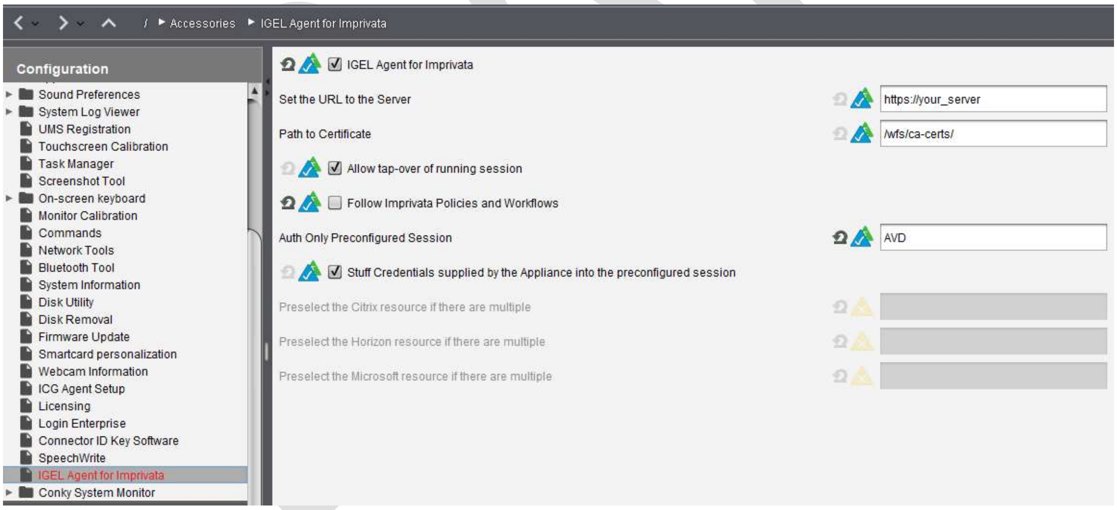
Authentication Only (Preconfigured Sessions)	Follow Imprivata Policies and Workflows (Roaming Sessions with Location Override)
IGEL OS 11.09.150	**IGEL OS 11.09.150**
Microsoft AVD • Roaming Desktops • Roaming Remote Apps Windows 365 Cloud PC Enterprise • Roaming Desktops • Uses the IGEL AVD app on OS 11 Microsoft RDP • Roaming Desktops	Microsoft RDSH / RDP • Apps or Desktops REQUIREMENT: • IGEL endpoint must have an Imprivata Computer Policy with VDA settings for Microsoft • End user must have an Imprivata User Policy with VDA enabled for Microsoft

7.0: Authentication Only Workflows

7.1: Basic Setup – IGEL Profile for Auth Only

NOTE: There are a few settings in the profile configuration UI and several that are in the IGEL Registry (see section 7.1.1).

1. In the profile configurator, go to **Accessories > IGEL Agent for Imprivata**.
2. Edit the profile parameter settings as follows:
    a. IGEL Agent for Imprivata = **enabled**
    b. Set the URL to the Server(s)
        i. Use FQDN format (Ex: **https://imprivata.company.net**)
            1. For multiple appliances, all appliances must be in the same Imprivata Enterprise
            2. List the appliance URL's separated by a semicolon with no spaces.
            3. Ex: **https://appliance1.company.net;https://appliance2.company.net**
    c. Path to Certificate = keep the default setting of **/wfs/ca-certs/**
    d. Allow tap-over of running session = **enabled (default)**
    e. Follow Policies and Workflows = **Uncheck this setting**
        i. This is not compatible with the Auth Only Preconfigured Session workflow
    f. Auth Only Preconfigured Session = **Enter the name of the preconfigured session**
        i. **See Sections 7.2 for setup instructions**
    g. Stuff Credentials supplied by the Appliance into the preconfigured session = **enabled (default)**
        i. **Do NOT disable this setting.**



/ ► Accessories ► IGEL Agent for Imprivata

☑ IGEL Agent for Imprivata

Set the URL to the Server: https://your_server

Path to Certificate: /wfs/ca-certs/

☑ Allow tap-over of running session

□ Follow Imprivata Policies and Workflows

Auth Only Preconfigured Session: AVD

☑ Stuff Credentials supplied by the Appliance into the preconfigured session

Preselect the Citrix resource if there are multiple

Preselect the Horizon resource if there are multiple

Preselect the Microsoft resource if there are multiple

7.1.1: IGEL Registry settings for Auth Only

Menu Path: System > Registry > iia

Parameter	Options / Default setting	Description Notes
allow_tapover	enable **(default)** / disable	Disconnect or logoff a session in progress to logon a new user.
auth_only_session	enable / **disable (default)** i.e. enter the name of the preconfigured session	**Requires a locally configured session: AVD, Citrix, VMWare, RDP** IMPORTANT: this setting is disabled if using the Follow Imprivata Policies workflow
bgimage	**default (default) /** appliance / manual edit	Related to the **lockscreen** setting but can also be used with the compact logon screen. Choose the background image - default is an IGEL background, Appliance uses the Imprivata Computer Policy setting for Customization. Manual edit – you can type the path to an image file that needs to be in the /wfs/ directory (ex: background.jpg)
exit_default.authonly	**logoff (default)** / disconnect	Setting for how to leave an Auth Only session when logging out of the agent (i.e. Tap Out or Tap Over). AVD sessions will always be disconnected.
hide_on_idle	enable **/ disable (default)**	**Hide the agent window after logging in when idle.**
lockscreen	enable **/ disable (default)**	Enables a full lock screen to hide the IGEL desktop You can use a hotkey (ESC + I) to toggle between the Full Lock Screen and the Compact logon (default)
stuff_cred	**enable (default)** / disable	Required for Auth Only – stuffs credentials supplied by the Appliance into the preconfigured session.

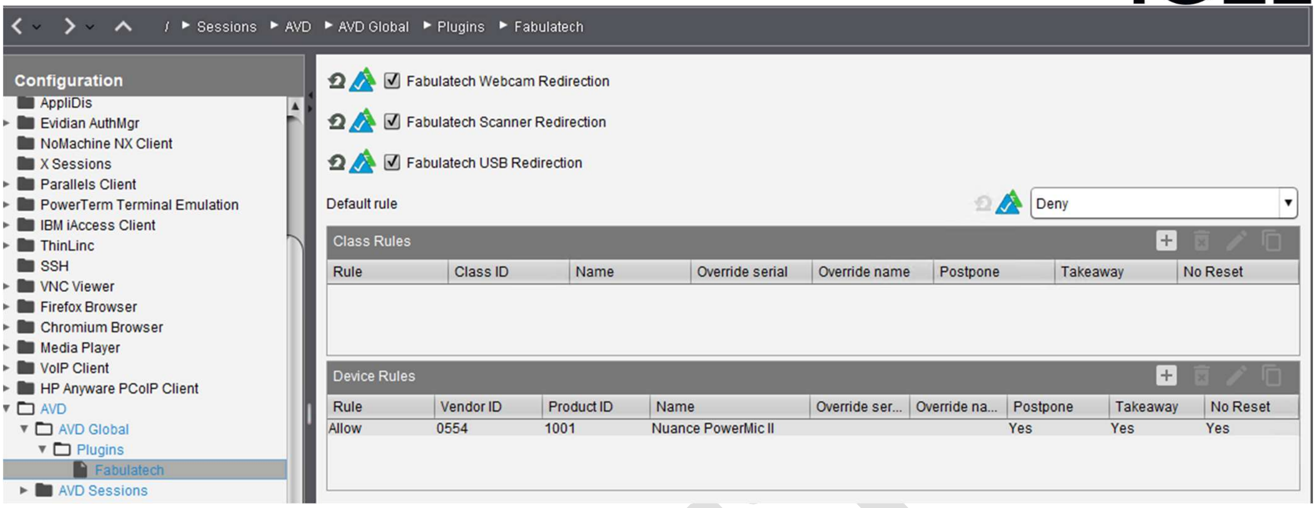
7.2: Preconfigured Session- Microsoft AVD or Windows 365 Cloud PC Enterprise

7.2.1 Supported Workflows:

- Roaming Desktops - AVD or Windows 365 Cloud PC Enterprise
  - W365 Cloud PC will use the IGEL AVD app
- Roaming AVD Remote Apps

7.2.2 IGEL Profile Setup

1. **AVD Global Settings > Plugins > Fabulatech** – see this: Fabulatech Redirection for AVD in IGEL OS
   a. Some customers will need support for peripherals like USB devices, Scanners and/or Webcams within the AVD session host or W365 session. IGEL supports Fabulatech integration via their plugins. Additional Fabulatech products that may be needed are Serial Port or Sound Redirection. These are available as IGEL OS Custom Partitions. Contact IGEL for more information.
   b. This is an example of using Fabulatech for USB redirection
      i. **RECOMMENDED:** Default rule = Deny
      ii. **Device rules** – Allow and specify the Vendor ID (VID) and Product ID (PID) per device.



☑ Fabulatech Webcam Redirection

☑ Fabulatech Scanner Redirection

☑ Fabulatech USB Redirection

Default rule: Deny

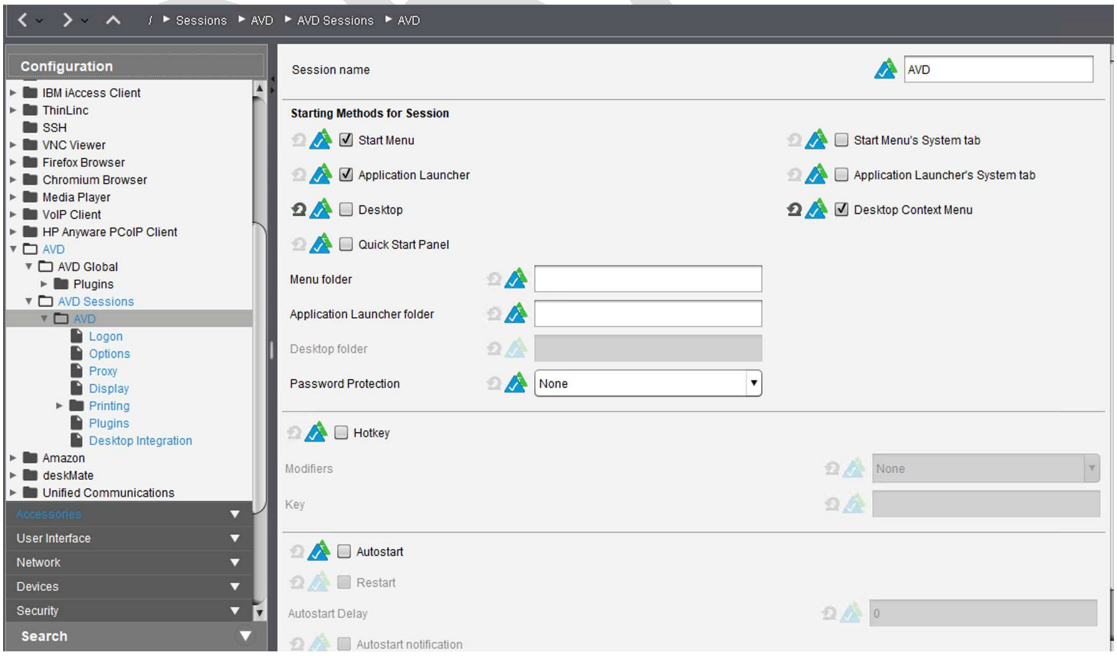
Class Rules

Rule	Class ID	Name	Override serial	Override name	Postpone	Takeaway	No Reset

Device Rules

Rule	Vendor ID	Product ID	Name	Override ser...	Override na...	Postpone	Takeaway	No Reset
Allow	0554	1001	Nuance PowerMic II			Yes	Yes	Yes

2. AVD Session Setup: In the profile configurator, go to **Sessions > AVD > AVD Sessions**.
3. Click the "+" button to add a preconfigured session – the session settings will appear.
    a. **REQUIRED:** Create a Session Name (**ex: AVD**)
        i. This name is used by IAFI for launching the Auth Only preconfigured session.
        ii. The session name must not contain any of these characters: \ / : * ? " < > | [ ] { } ( )
    b. **OPTIONAL:** Modify the Starting Methods for session
        i. Since the IGEL Agent for Imprivata is controlling the start of the session, we recommend removing the Desktop icon option.
        ii. The other choices would be good in a DR scenario. (ex: Imprivata Appliances are down and you need to manually start a session)
    c. **REQUIRED:**
        i. Hotkey, Autostart, Restart – leave these disabled (default)



Session name: AVD

Starting Methods for Session

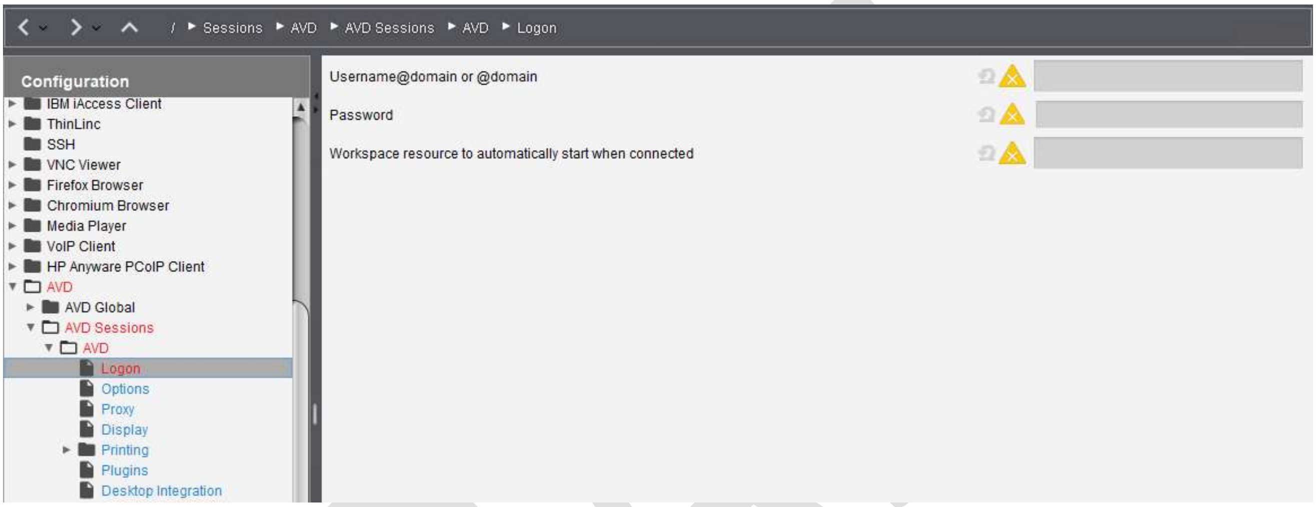
☑ Start Menu
☐ Start Menu's System tab
☑ Application Launcher
☐ Application Launcher's System tab
☐ Desktop
☑ Desktop Context Menu
☐ Quick Start Panel

Menu folder:
Application Launcher folder:
Desktop folder:
Password Protection: None

☐ Hotkey
Modifiers: None
Key:

☐ Autostart
☐ Restart
Autostart Delay: 0
☐ Autostart notification

4. Logon setting
    a. **REQUIRED:** Leave the Username, Password parameter fields blank (default).
        i. Do not enable these settings as the agent uses them when we get credentials from the appliance.
    b. **OPTIONAL:** Workspace resource to automatically start when connected
        i. If the user only has one AVD entitlement assigned (desktop or app) or W365 desktop, you don't need to specify the resource name. It will automatically launch after we authenticate to the Azure broker. This behavior is controlled by the "autostartsingle" IGEL registry setting. See section 7.2.3

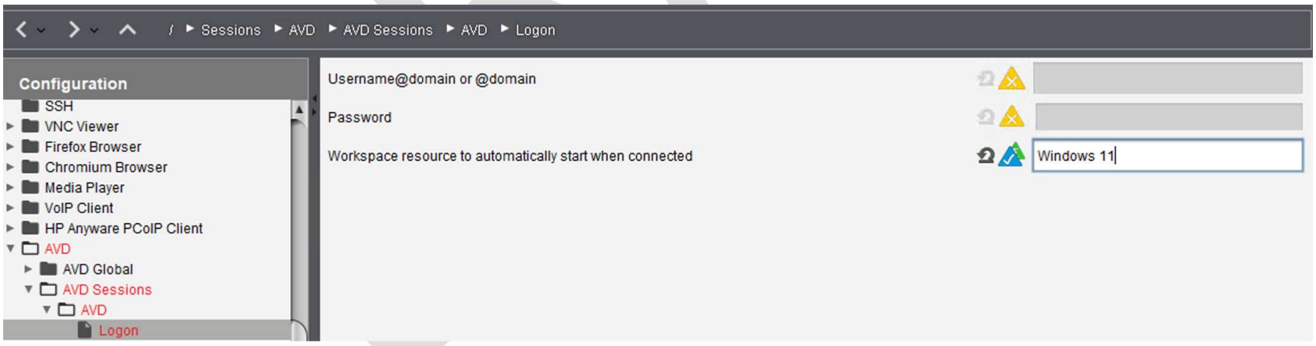


Username@domain or @domain

Password

Workspace resource to automatically start when connected

        ii. If the user has multiple AVD desktop/app or W365 resources and you want one of them to automatically launch, specify the name of that resource in this field (ex: Windows 11)



Username@domain or @domain

Password

Workspace resource to automatically start when connected: Windows 11

5. Additional AVD Session settings (Options, Proxy, Display, Printing, Plugins) are based on customer requirements. See the IGEL KB for more information on these AVD settings.

7.2.3 Additional IGEL Registry settings for AVD sessions

These are a few settings to note that should be reviewed when creating your AVD session.

Menu Path: System > Registry > sessions > wvd(some number) > options

Parameter	Options / Default setting	Description Notes

autostartsingle	**enable (default)** / disable	Autostart a single session if that is the only resource for a user. This is the default option and should not be changed
background-image	enable / **disable (default)** i.e. enter the path of an image file	From UMS, deploy a custom image (.jpg) into the /wfs directory and specify the path here to change the default AVD client background image.
cache-username	**enable (default)** / disable	Disable this setting so the username field will always be blank in the AVD client session.
client-log-level	**Critical (default)** / Error / Warning / Info / Debug / Trace	AVD client log level settings. Change from the default at the direction of IGEL support when troubleshooting is needed.
compact-login-view	enable **/ disable (default)**	Show compact version of the AAD login. Enable this option as it can potentially solve AAD incompatibilities with QTWebEngine where login might hang randomly.
http-user-agent	**System Default (default) /** Windows / Android / iOS / macOS / manual edit	System default will indicate the AVD session is coming from a Linux device. You should not need to modify this but the option exists for a manual edit if a customer needs a custom user agent string. We do not recommend changing to the other options.
udp-short-path	enable **/ disable (default)**	UDP Short Path – enable for customers using this option with their AVD sessions.
no-background	enable **/ disable (default)**	Enable if you don’t want any background image for the AVD session when it starts.

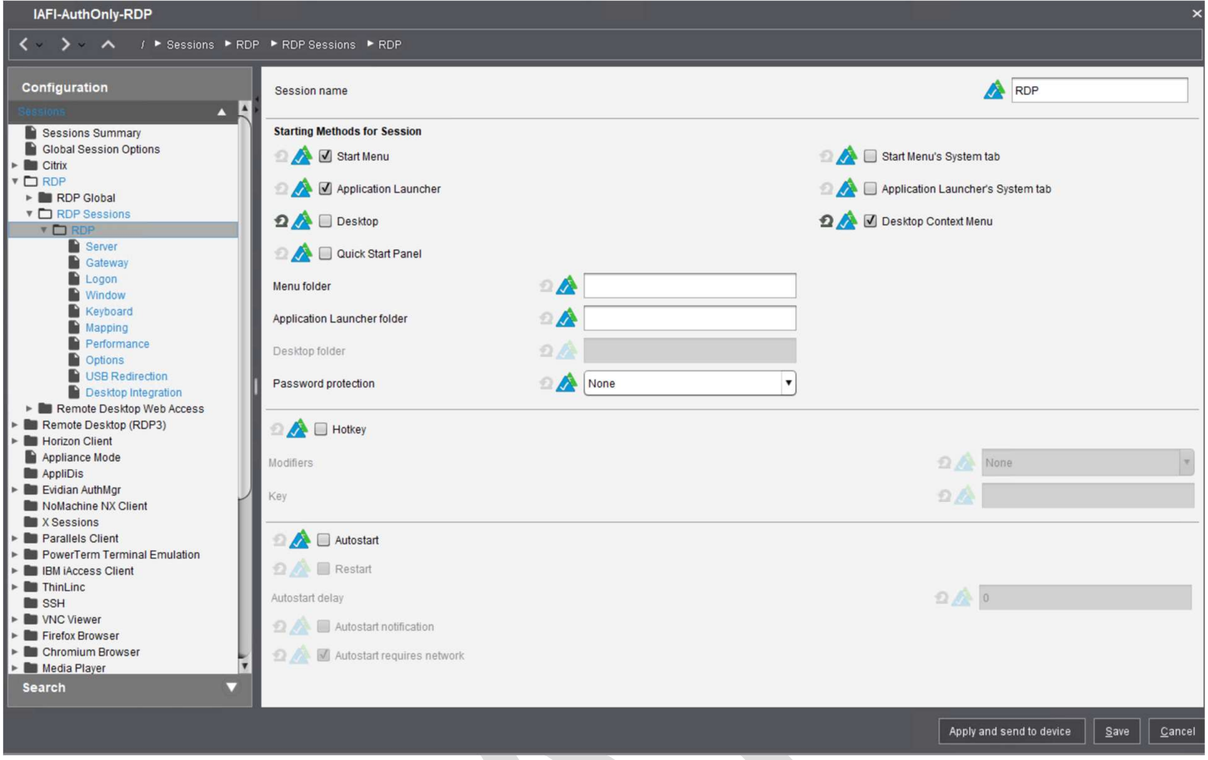
7.3: Microsoft RDP Preconfigured session

7.3.1 Supported Use Cases:

- RDP / RDSH Roaming desktop session

7.3.2 IGEL Profile Setup

1. **RDP Global Settings > Gateway**
    a. **Don’t use Gateway support**
    b. Other options are based on customer needs
4. RDP Session Setup: In the profile configurator, go to **Sessions > RDP > RDP Sessions**.
5. Click the “+” button to add a preconfigured session – the session settings will appear.
    a. **REQUIRED:** Create a Session Name (**ex: RDP**)
        i. This name is used by IAFI for launching the Auth Only preconfigured session.
        ii. The session name must not contain any of these characters: \ / : * ? “ < > | [ ] { } ( )
    b. **OPTIONAL:** Modify the Starting Methods for session
        i. Since the IGEL Agent for Imprivata is controlling the start of the session, we recommend removing the Desktop icon option.
        ii. The other choices would be good in a DR scenario. (ex: Imprivata Appliances are down and you need to manually start a session)
    c. **REQUIRED:**
        i. Hotkey, Autostart, Restart – leave these disabled (default)



Session name: RDP

Starting Methods for Session

☑ Start Menu
☐ Start Menu's System tab
☑ Application Launcher
☐ Application Launcher's System tab
☐ Desktop
☑ Desktop Context Menu
☐ Quick Start Panel

Menu folder:

Application Launcher folder:

Desktop folder:

Password protection: None

☐ Hotkey

Modifiers: None

Key:

☐ Autostart

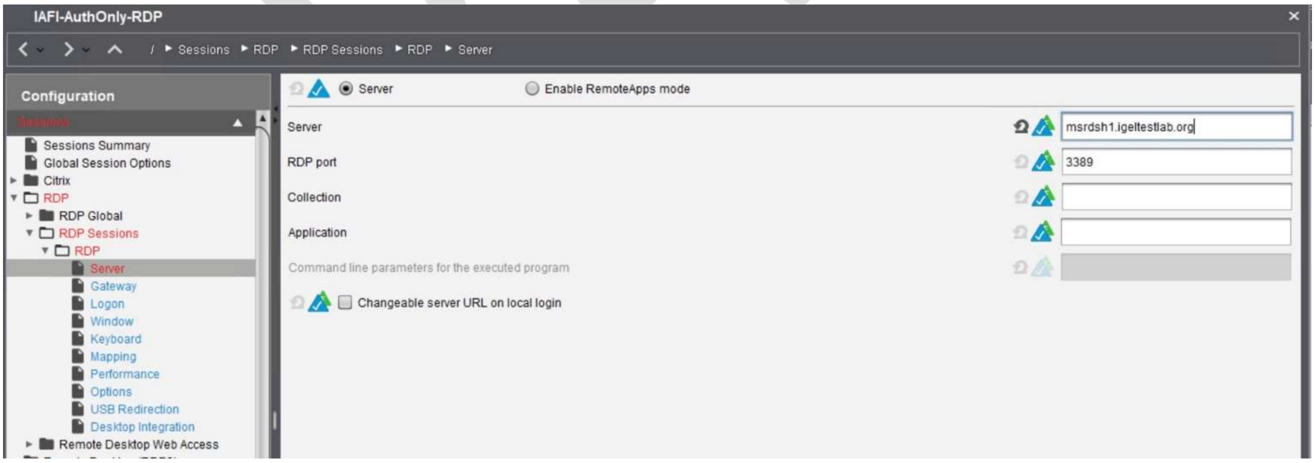
☐ Restart

Autostart delay: 0

☐ Autostart notification

☑ Autostart requires network

6. Server setting
    a. **REQUIRED:** Enter the IP address or hostname for the connection
    b. RDP port: Default is 3389. Change only if the server is using another port



● Server ○ Enable RemoteApps mode

Server: msrdsh1.igeltestlab.org

RDP port: 3389

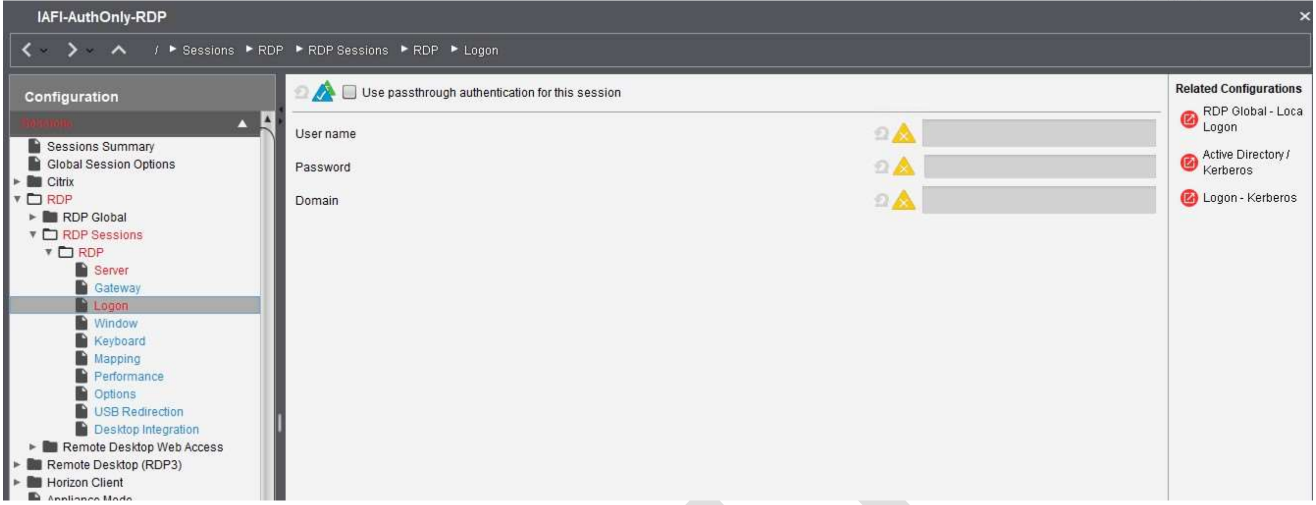
Collection:

Application:

Command line parameters for the executed program:

☐ Changeable server URL on local login

7. Logon setting
    a. **REQUIRED:** Leave the Username, Password parameter fields blank (default).
        i. Do not enable these settings as the agent uses them when we get credentials from the appliance.
        ii. Do not enable passthrough authentication for this session



□ Use passthrough authentication for this session

User name

Password

Domain

8. Additional RDP Session settings (Window, Keyboard, Mapping, etc.) are based on customer requirements. See the IGEL KB for more information on these RDP session settings.

7.4: Imprivata User/Computer Policy settings

For an Authentication Only workflow, the IGEL Agent for Imprivata won't use the VDA Computer or User policy settings to automate the workflow. We still check for VDA licenses assigned to the user policy as that is a requirement.

7.4.1: User Policy setup – Auth Only workflow

- **Authentication**
  - **Desktop Access authentication – Primary factors**
    - SUPPORTED: Password (no second factor)
    - SUPPORTED: Proximity Card (no second factor, Password or Imprivata PIN)
    - All other primary auth methods are not supported at this time
  - **Authentication method options**
    - SUPPORTED: Imprivata PIN options
    - SUPPORTED: Proximity Card options
      - Allow unlimited cards or pick a number
      - Grace period for second authentication factor
- **Challenges**
  - not yet supported
- **Self-Service Password/Imprivata PIN Reset**
  - OPTIONAL: Q&A enrollment is supported
  - NOT SUPPORTED: SSPR via the agent login
  - NOT SUPPORTED: Imprivata PIN Reset
- **Single Sign-On**
  - OPTIONAL: Can be enabled with the default options but IAFI doesn't require it
- **Virtual Desktops**
  - **REQUIRED:** this must be enabled: Enable virtual desktop access automation
    - All other VDA user policy settings are ignored in Auth Only mode

7.4.2: Computer Policy setup – Auth Only workflows

These computer policy settings are used / supported in Auth Only mode

- **General**
  - Card Readers – Imprivata branded / rfIdeas models
    - Beep card reader when user taps card
    - Configuration settings for programmable readers
  - NOTE: these settings will be applied when the agent starts, the reader is plugged in.
- **No Settings Used**
  - Shared Workstation
  - Walk-Away Security
  - Virtual Desktops– IAFI ignores the VDA workflow options
  - Citrix or Terminal Server
  - Fingerprint
  - Extensions
- **Connector for Epic**
  - Multi-App – Log out or Secure Epic when endpoint is locked
- **Override and Restrict**
  - Desktop Access Authentication Restrictions – these can be applied to restrict certain authentication methods to the endpoint
- **Customization**
  - Background image is supported
  - Login Authentication Prompts
    - Enter Proximity card prompt
    - Enter credential prompt
  - Proximity card prompt image
  - Username and password text

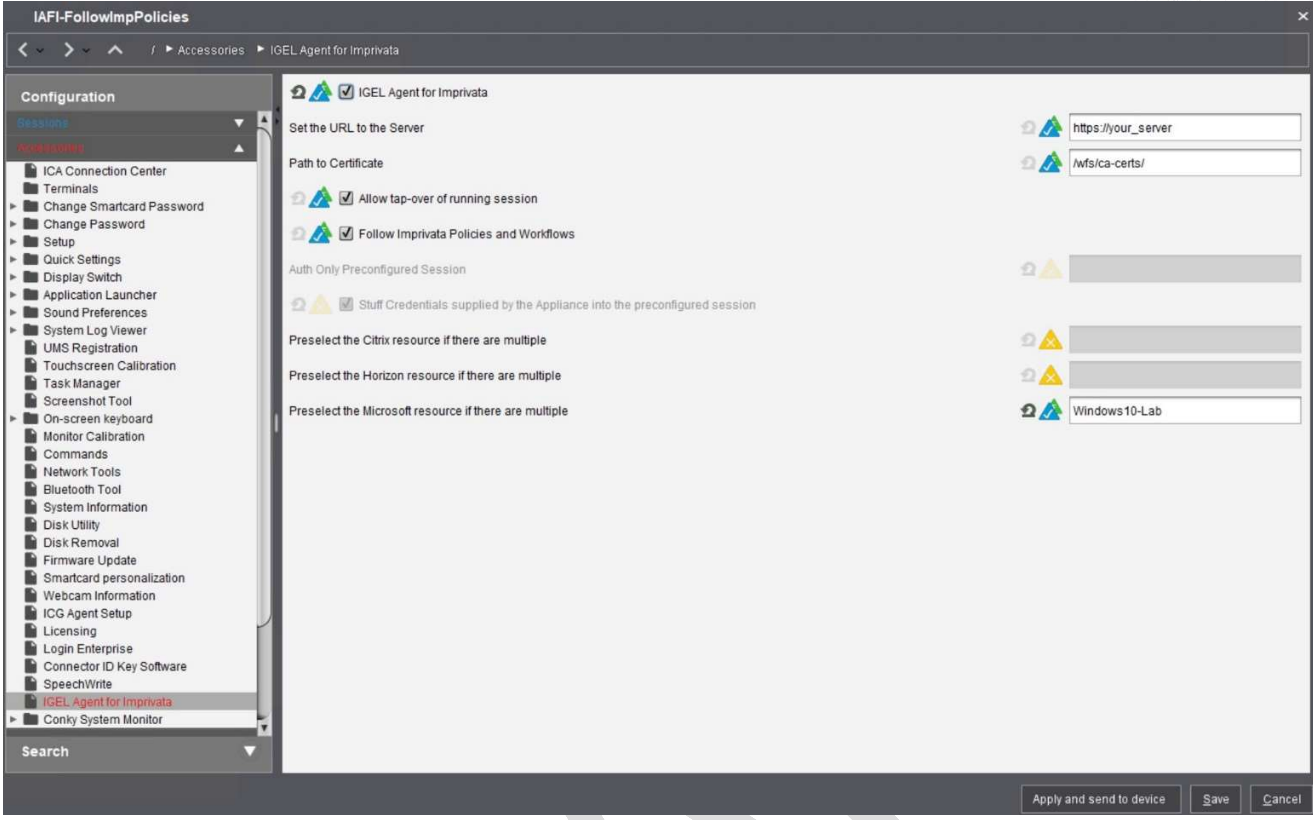
8.0: Follow Imprivata Policies and Workflows

Like the Imprivata PIE agent, this workflow requires the correct Imprivata VDA Computer and User policy settings to be properly setup for the supported Microsoft Remote Desktop Services workflows. This configuration does not use an IGEL preconfigured session like the Authentication Only option.

- The IGEL Agent for Imprivata endpoint will register as a computer in the appliance and must have a Computer policy setting with VDA enabled for the Microsoft workflow(s).
- The user must have an Imprivata policy setting with VDA enabled for the supported Microsoft Remote Desktop Services workflow.

IGEL - Location Based Override

Additionally, the IGEL Agent for Imprivata agent setup has an option to provide a Location Based override to launch a specific desktop resource if there are multiple. This feature bypasses the Imprivata Computer Policy setting to “prompt” a user with a chooser displaying multiple desktop resources if the user is entitled to them.



☑ IGEL Agent for Imprivata

Set the URL to the Server: https://your_server

Path to Certificate: /wfs/ca-certs/

☑ Allow tap-over of running session

☑ Follow Imprivata Policies and Workflows

Auth Only Preconfigured Session

☑ Stuff Credentials supplied by the Appliance into the preconfigured session

Preselect the Citrix resource if there are multiple

Preselect the Horizon resource if there are multiple

Preselect the Microsoft resource if there are multiple: Windows10-Lab

IGEL Override for RDP session

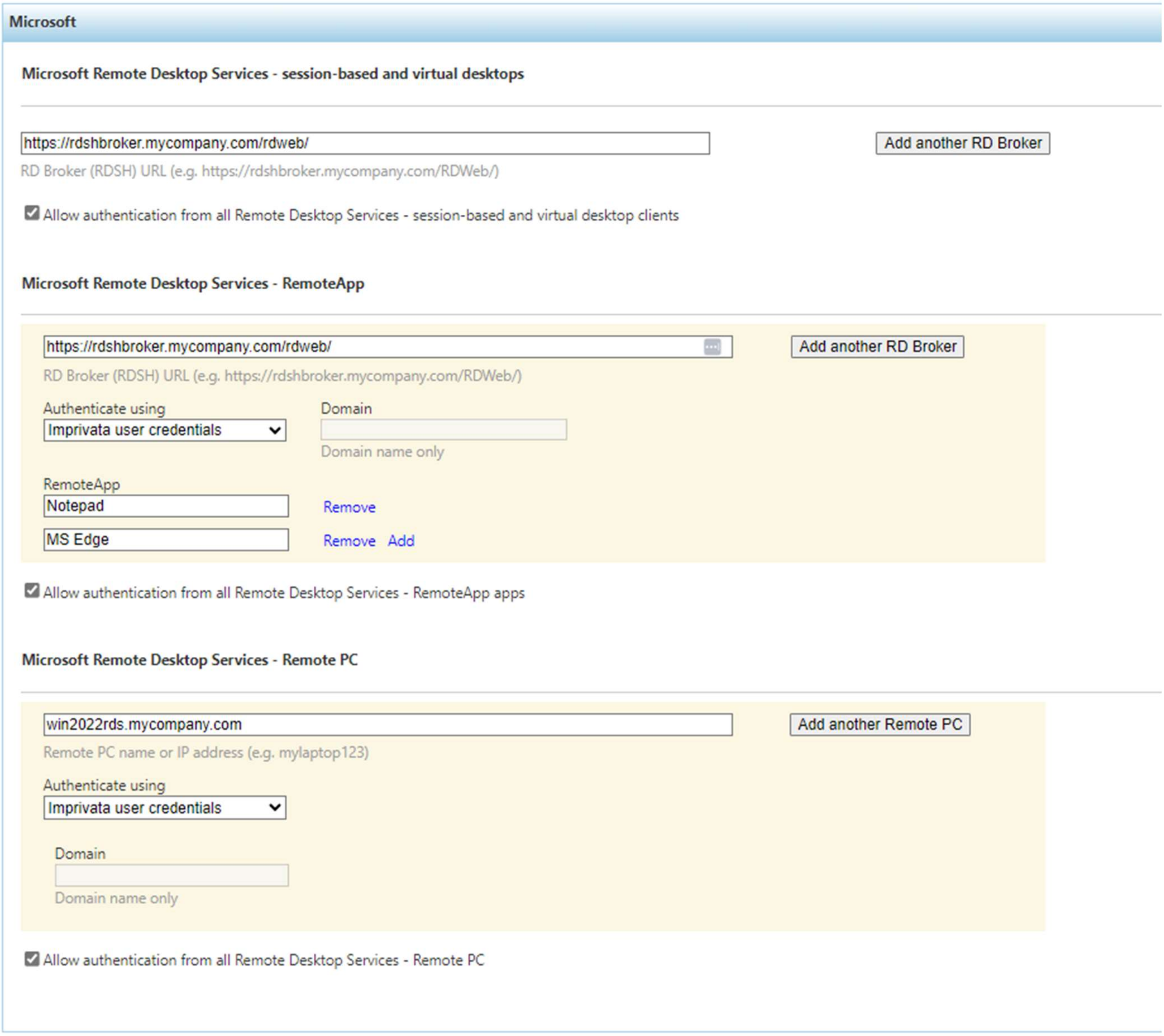
8.1: Imprivata Appliance Setup

8.1.1: Configure Virtual Desktop Broker URL’s

To use the Imprivata Microsoft RDSH / Remote PC settings with this configuration, you need to specify the RDSH broker URL(s) or Remote PC name/IP address within the OneSign Appliance Web Console.

1. Log into the Imprivata OneSign Server Web Console as an administrator.
2. On the top level menu, select **Computers** and on the drop down menu, click the **Virtual desktops** option.
3. Add the Virtual Desktop broker URLs and/or Remote PC hostname or IP address in the respective sections
    a. Microsoft Remote Desktop Services – session-based and virtual desktops
    b. Microsoft Remote Desktop Services – Remote App
    c. Microsoft Remote Desktop Services - Remote PC
4. Select the Allow authentication from devices check box for the respective VDI brokers.
5. Save your settings.

This is an example of the Imprivata Virtual Desktop Broker settings for Microsoft.



Microsoft

Microsoft Remote Desktop Services - session-based and virtual desktops

https://rdshbroker.mycompany.com/rdweb/

RD Broker (RDSH) URL (e.g. https://rdshbroker.mycompany.com/RDWeb/)

☑ Allow authentication from all Remote Desktop Services - session-based and virtual desktop clients

Microsoft Remote Desktop Services - RemoteApp

https://rdshbroker.mycompany.com/rdweb/

RD Broker (RDSH) URL (e.g. https://rdshbroker.mycompany.com/RDWeb/)

Authenticate using: Imprivata user credentials

Domain:

Domain name only

RemoteApp: Notepad

MS Edge

☑ Allow authentication from all Remote Desktop Services - RemoteApp apps

Microsoft Remote Desktop Services - Remote PC

win2022rds.mycompany.com

Remote PC name or IP address (e.g. mylaptop123)

Authenticate using: Imprivata user credentials

Domain:

Domain name only

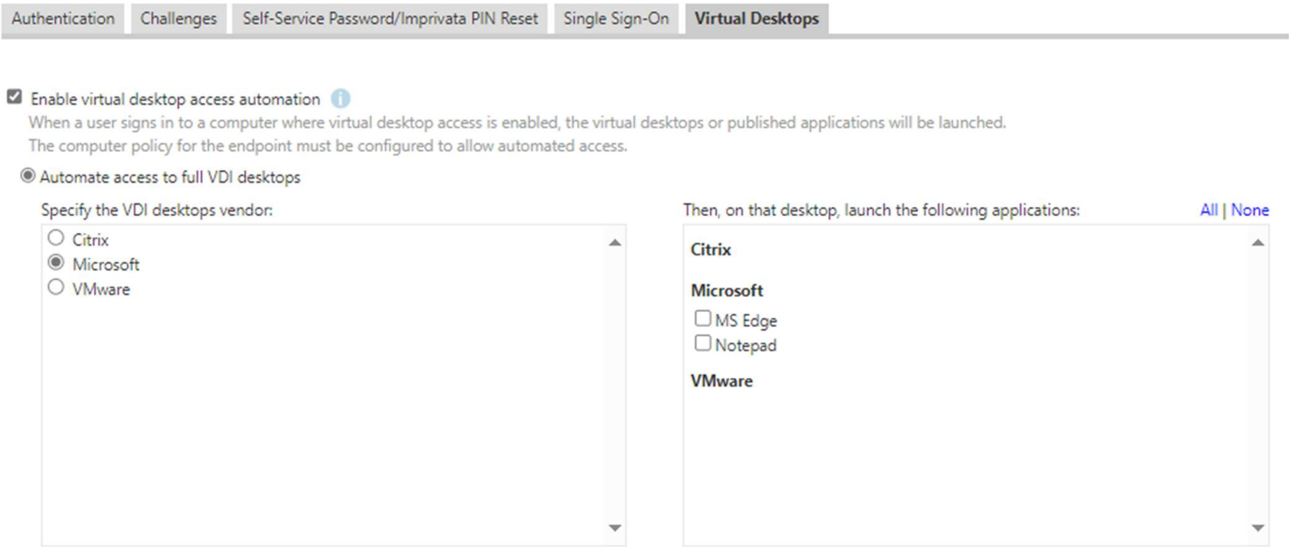
☑ Allow authentication from all Remote Desktop Services - Remote PC

8.1.2: User Policy setup – Follow Policies workflow

- **Authentication**
  - **Desktop Access authentication – Primary factors**
    - SUPPORTED: Password (no second factor)
    - SUPPORTED: Proximity Card (no second factor, Password or Imprivata PIN)
    - All other primary auth methods are not supported at this time
  - **Authentication method options**
    - SUPPORTED: Imprivata PIN options
    - SUPPORTED: Proximity Card options
      - Allow unlimited cards or pick a number
      - Grace period for second authentication factor
- **Challenges**

- not yet supported

- **Self-Service Password/Imprivata PIN Reset**
  - OPTIONAL: Q&A enrollment is supported
  - NOT SUPPORTED: SSPR via the agent login
  - NOT SUPPORTED: Imprivata PIN Reset
- **Single Sign-On**
  - OPTIONAL: Can be enabled with the default options but IAFI doesn't require it
- **Virtual Desktops**
  - **REQUIRED:** this must be enabled: Enable virtual desktop access automation
  - **Options:**
    - Automate access to full VDI desktops – **Select Microsoft**
    - Automate access to Remote PC



☑ Enable virtual desktop access automation

When a user signs in to a computer where virtual desktop access is enabled, the virtual desktops or published applications will be launched.
The computer policy for the endpoint must be configured to allow automated access.

● Automate access to full VDI desktops

Specify the VDI desktops vendor:

○ Citrix
● Microsoft
○ VMware

Then, on that desktop, launch the following applications: All | None

Citrix

Microsoft

□ MS Edge
□ Notepad

VMware

8.1.3: Computer Policy Setup – Follow Policies Workflow

These computer policy settings are used / supported in Follow Policies mode

- **General**
  - Card Readers – Imprivata branded / rfIdeas models
    - Beep card reader when user taps card
    - Configuration settings for programmable readers
  - NOTE: these settings will be applied when the agent starts, the reader is plugged in.
- **Virtual Desktops**
  - **Microsoft Remote Desktop Services – session based and virtual desktops**
    - **Automate access – must be enabled if using a MS broker**
    - **Available RD brokers – one must be selected**
  - **Microsoft Remote Desktop Services – Remote PC**
    - **Automate access – must be enabled if using this option**
- **No Settings Used**
  - Shared Workstation

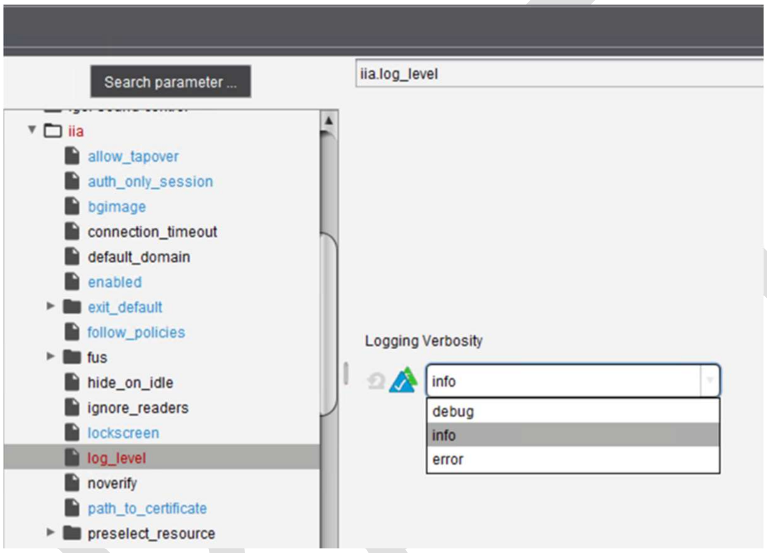
- Walk-Away Security
- Citrix or Terminal Server
- Fingerprint
- Extensions

- **Connector for Epic**
  - Multi-App – Log out or Secure Epic when endpoint is locked
- **Override and Restrict**
  - Desktop Access Authentication Restrictions – these can be applied to restrict certain authentication methods to the endpoint
- **Customization**
  - Background image is supported
  - Login Authentication Prompts
    - Enter Proximity card prompt
    - Enter credential prompt
  - Proximity card prompt image
  - Username and password text

Appendix A: How to enable and capture logs for troubleshooting

Create a profile to enable the advanced logging levels

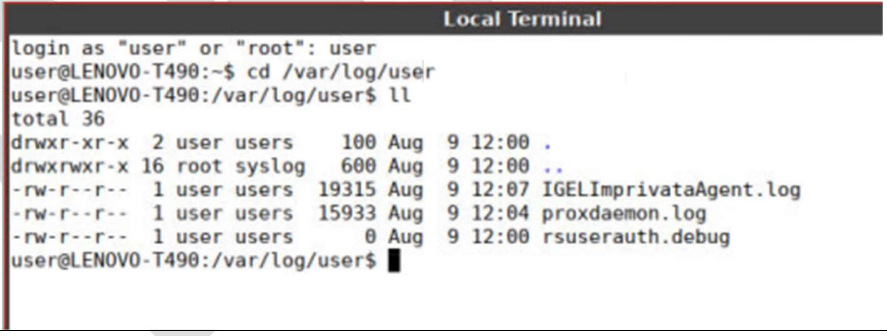
1. In the profile configurator, go to **System > Registry > iia > log_level**.
2. Modify the settings to switch to debug or error log levels:
   a. Options: info (**default**), debug, error
   b. **IMPORTANT**: Do not leave debug or error logging on continuously. It should only be enabled for troubleshooting and removed when completed. Switch back to **info** logging for normal production use.
3. Save the profile and apply to the device/folder as needed



iia.log_level

Logging Verbosity: info

<table>
<tr><td><b>Log location</b></td><td><b>/var/log/user</b>



```
login as "user" or "root": user
user@LENOVO-T490:~$ cd /var/log/user
user@LENOVO-T490:/var/log/user$ ll
total 36
drwxr-xr-x  2 user users    100 Aug  9 12:00 .
drwxrwxr-x 16 root syslog   600 Aug  9 12:00 ..
-rw-r--r--  1 user users  19315 Aug  9 12:07 IGELImprivataAgent.log
-rw-r--r--  1 user users  15933 Aug  9 12:04 proxdaemon.log
-rw-r--r--  1 user users      0 Aug  9 12:00 rsuserauth.debug
user@LENOVO-T490:/var/log/user$ 
```

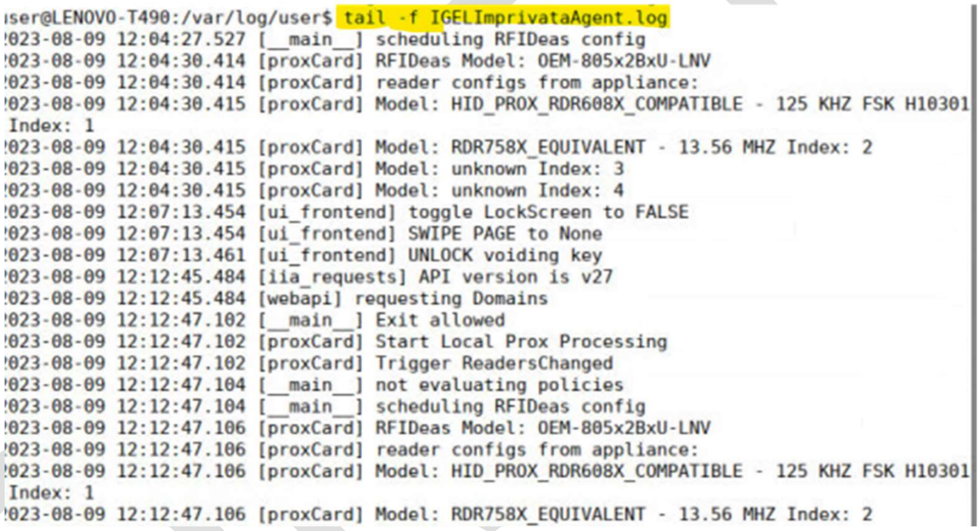
</td></tr>
<tr><td rowspan="3"><b>Log Files</b></td><td><b>IGELImprivataAgent.log</b>
• Main agent/appliance activity log</td></tr>
<tr><td><b>Proxdaemon.log</b>
• RFIdeas reader log. Will show activity with the prox reader</td></tr>
<tr><td><b>IGELImprivataAgentERR.log</b>
• Only seen if an agent crash occurs</td></tr>
</table>

How to live monitor the log files while troubleshooting.

NOTE: This requires the log level to be in debug mode

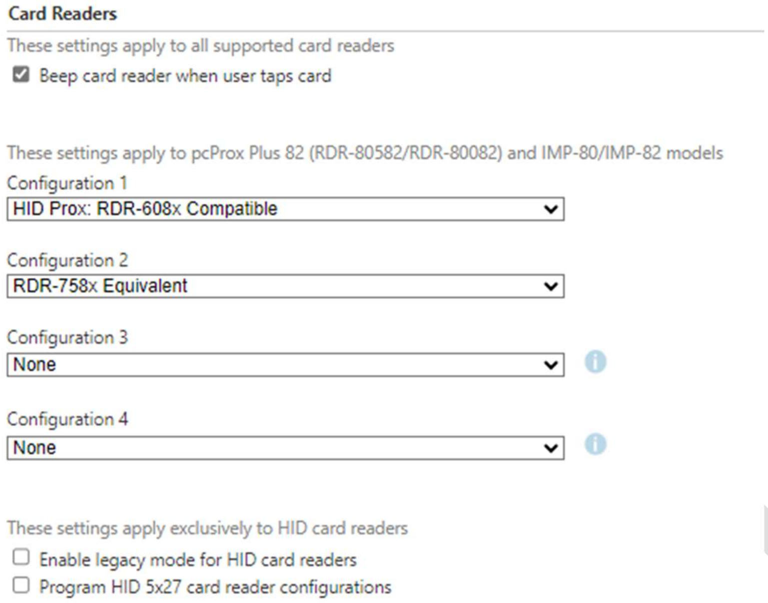
Tailing the Log files

1. Create a profile for a local terminal or use a remote terminal session
2. Open the terminal session and **change to the user context**
    a. If logged in as root, type: “**su user**” to change to the user context
3. At the command line, type **/var/log/user** and hit the **Enter** key
4. Type “**ls**” to see the contents of the directory
    a. You should see the **IGELImprivataAgent.log** file
5. Type “**tail -f IGELImprivataAgent.log**” and hit **Enter**
    a. You should see live activity in the log file as you authenticate or use the agent system tray icon menu options like “**Sync**”



```
ser@LENOVO-T490:/var/log/user$ tail -f IGELImprivataAgent.log
023-08-09 12:04:27.527 [__main__] scheduling RFIDeas config
023-08-09 12:04:30.414 [proxCard] RFIDeas Model: OEM-805x2BxU-LNV
023-08-09 12:04:30.414 [proxCard] reader configs from appliance:
023-08-09 12:04:30.415 [proxCard] Model: HID_PROX_RDR608X_COMPATIBLE - 125 KHZ FSK H10301
 Index: 1
023-08-09 12:04:30.415 [proxCard] Model: RDR758X_EQUIVALENT - 13.56 MHZ Index: 2
023-08-09 12:04:30.415 [proxCard] Model: unknown Index: 3
023-08-09 12:04:30.415 [proxCard] Model: unknown Index: 4
023-08-09 12:07:13.454 [ui_frontend] toggle LockScreen to FALSE
023-08-09 12:07:13.454 [ui_frontend] SWIPE PAGE to None
023-08-09 12:07:13.461 [ui_frontend] UNLOCK voiding key
023-08-09 12:12:45.484 [iia_requests] API version is v27
023-08-09 12:12:45.484 [webapi] requesting Domains
023-08-09 12:12:47.102 [__main__] Exit allowed
023-08-09 12:12:47.102 [proxCard] Start Local Prox Processing
023-08-09 12:12:47.102 [proxCard] Trigger ReadersChanged
023-08-09 12:12:47.104 [__main__] not evaluating policies
023-08-09 12:12:47.104 [__main__] scheduling RFIDeas config
023-08-09 12:12:47.106 [proxCard] RFIDeas Model: OEM-805x2BxU-LNV
023-08-09 12:12:47.106 [proxCard] reader configs from appliance:
023-08-09 12:12:47.106 [proxCard] Model: HID_PROX_RDR608X_COMPATIBLE - 125 KHZ FSK H10301
 Index: 1
023-08-09 12:12:47.106 [proxCard] Model: RDR758X_EQUIVALENT - 13.56 MHZ Index: 2
```

6. OPTIONAL: Monitoring the RFIdeas proximity card daemon
    a. Type “**tail -f proxdaemon.log**” and hit **Enter**
    b. You should see information about the configuration assigned to the proximity reader from the **Imprivata Computer Policy – General Tab – Card Readers** section



Card Readers

These settings apply to all supported card readers

☑ Beep card reader when user taps card

These settings apply to pcProx Plus 82 (RDR-80582/RDR-80082) and IMP-80/IMP-82 models

Configuration 1: HID Prox: RDR-608x Compatible

Configuration 2: RDR-758x Equivalent

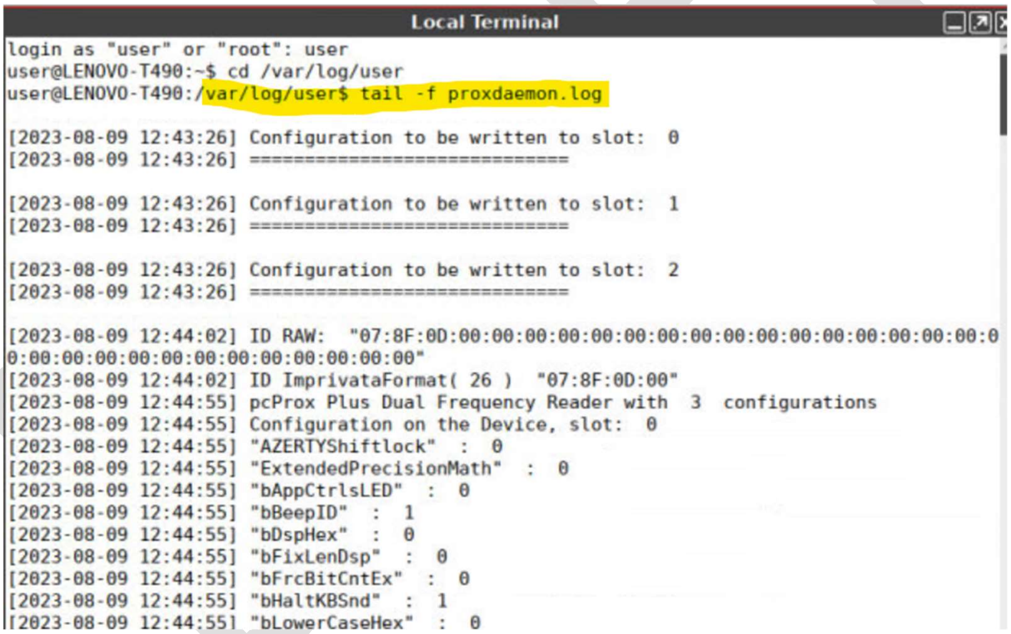
Configuration 3: None

Configuration 4: None

These settings apply exclusively to HID card readers

☐ Enable legacy mode for HID card readers

☐ Program HID 5x27 card reader configurations



Local Terminal

```
login as "user" or "root": user
user@LENOVO-T490:~$ cd /var/log/user
user@LENOVO-T490:/var/log/user$ tail -f proxdaemon.log

[2023-08-09 12:43:26] Configuration to be written to slot:  0
[2023-08-09 12:43:26] ==============================

[2023-08-09 12:43:26] Configuration to be written to slot:  1
[2023-08-09 12:43:26] ==============================

[2023-08-09 12:43:26] Configuration to be written to slot:  2
[2023-08-09 12:43:26] ==============================

[2023-08-09 12:44:02] ID RAW:  "07:8F:0D:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:0
0:00:00:00:00:00:00:00:00:00:00:00:00"
[2023-08-09 12:44:02] ID ImprivataFormat( 26 )  "07:8F:0D:00"
[2023-08-09 12:44:55] pcProx Plus Dual Frequency Reader with  3  configurations
[2023-08-09 12:44:55] Configuration on the Device, slot:  0
[2023-08-09 12:44:55] "AZERTYShiftlock"  :  0
[2023-08-09 12:44:55] "ExtendedPrecisionMath"  :  0
[2023-08-09 12:44:55] "bAppCtrlsLED"  :  0
[2023-08-09 12:44:55] "bBeepID"  :  1
[2023-08-09 12:44:55] "bDspHex"  :  0
[2023-08-09 12:44:55] "bFixLenDsp"  :  0
[2023-08-09 12:44:55] "bFrcBitCntEx"  :  0
[2023-08-09 12:44:55] "bHaltKBSnd"  :  1
[2023-08-09 12:44:55] "bLowerCaseHex"  :  0
```

Saving the log files for support

Option 1	From UMS – use the "Save device files for support" feature
Option 2	From a terminal, run this command: "**/config/bin/create_support_information**" This will create a zip file in **/tmp** that can be pulled off the device and added to a support case

Opening a support case

1. Log into the IGEL Customer Service Support Portal to open a case
   a. Provide IGEL OS version
   b. VDI Session Type (ex: AVD, Citrix, VMWare, etc.)
   c. Name the case: IGEL Agent for Imprivata – issue description
   d. Attach the log files to the case along with any pictures or videos of the issue

Appendix B: IGEL- Imprivata Feature Matrix

Updates: February 2024

Primary Authentication Methods	**Imprivata Windows Agent**	**Imprivata PIE Agent**	**IGEL Agent for Imprivata**	**Notes - IAFI**
Password	Yes	Yes	**Yes**	
Proximity Card	Yes	Yes	**Yes**	Imprivata Branded / rf IDEAS readers
Smart Card	Yes	Yes		
FIDO Security Key	Yes	Yes		
Fingerprint Biometrics	Yes	Yes		
Question and Answer	Yes	Yes		

Primary Authentication Workflows	**Imprivata Windows Agent**	**Imprivata PIE Agent**	**IGEL Agent for Imprivata**	**Notes - IAFI**
Password	Yes	Yes	Yes	
Password + Change PW (expired password)	Yes	Yes	Yes	
Password + Change PW (new PW invalid)	Yes	Yes	Yes	
Enroll Proximity Card	Yes	Yes	Yes	
Proximity Card Alone (Retrieve Password)	Yes	Yes	Yes	
Proximity Card + Password or Expired / Change PW	Yes	Yes	Yes	
Proximity Card + Imprivata PIN	Yes	Yes	Yes	
Proximity Card + Enroll Imprivata PIN	Yes	Yes	Yes	
Tap to Lock Endpoint	Yes	Yes	Yes	
Tap to Switch Users / Tap Over	Yes	Yes	Yes	
Hotkey to Lock Endpoint	Yes	Yes		

Authentication/ Reauthentication Methods via Virtual Channel	**Imprivata Windows Agent**	**Imprivata PIE Agent**	**IGEL Agent for Imprivata**	**Notes - IAFI**
Proximity Card	Yes	Yes	Yes	
Smart Card	Yes			
FIDO Security Key	Yes			
Fingerprint Biometrics	Yes	Yes		
Imprivata Hands Free Authentication	Yes	Yes		

General Features and Workflows	**Imprivata Windows Agent**	**Imprivata PIE Agent**	**IGEL Agent for Imprivata**	**Notes - IAFI**
Minimum Windows OS or IGEL OS Version	See Imprivata Supported Components Guide	See Imprivata Supported Components Guide	IGEL OS 11.09.150	Also available in 11.08.440 and 11.09.100
Appliance Failover	Yes	Yes	Yes	List the appliance URL's separated by a semicolon. All appliances must be in the same Imprivata Enterprise. You can vary the connection timeout by seconds. Default is 5 sec before a failover switch.
Offline Mode	Yes	Yes		
Self-Service Password Reset (via agent login screen)	Yes	Yes		Roadmap
Third-party Self-Service Password Reset (via agent login screen)	Yes	Yes		Roadmap
Non-OneSign User Workflow	Yes	Yes	Yes	
Spine Combined Workflow (NHS)	Yes	Yes		TBD
Smartcard as Proximity	Yes	Yes		TBD

Card Workflow				
Customization Objects (Computer Policy)	Yes	Yes	Yes	Custom Wallpaper, Prox Badge image, Logon text

Walk-Away Security	Imprivata Windows Agent	Imprivata PIE Agent	IGEL Agent for Imprivata	Notes - IAFI
Honors Lock Command (Hotkey)	Yes	Yes		
Fade to Lock Screensaver	Yes	Yes		
Notification Balloon	Yes	Yes		
Secure Walk-Away (via Imprivata BLE Dongle)	Yes	Yes		

Microsoft Workflows	Imprivata Windows Agent	Imprivata PIE Agent	IGEL Agent for Imprivata	Notes - IAFI
Azure Virtual Desktops (AVD)			Yes	Auth Only Mode
Azure Virtual Desktop Apps			Yes	Auth Only Mode (Experimental)
Windows 365 Cloud PC Enterprise			Yes	Auth Only Mode
Windows 365 Cloud PC Frontline Worker				Roadmap
Virtual Kiosk for AVD/Win 365 Cloud PC				Roadmap
RDS/Remote PC Desktops	Yes	Yes	Yes	Follow Policies or Auth Only Mode
RDS Applications	Yes			
Virtual Kiosk for RDS/Remote PC Desktops	Yes			Roadmap
Virtual Kiosk for RDS Published Applications	Yes			

Citrix Workflows	Imprivata Windows Agent	Imprivata PIE Agent	IGEL Agent for Imprivata	Notes - IAFI
Virtual Desktops (on-prem)	Yes	Yes	Yes	Follow Policies or Auth Only mode
Virtual Apps (on-prem)	Yes	Yes	Yes	Follow Policies or Auth Only Mode
Virtual Desktops (Cloud)	Yes	Yes	Yes	Auth Only Mode
Virtual Apps (Cloud)	Yes	Yes	Yes	Auth Only Mode

VMWare Workflows	Imprivata Windows Agent	Imprivata PIE Agent	IGEL Agent for Imprivata	Notes - IAFI
Virtual Desktops (on-prem)	Yes	Yes	Yes	Follow Policies or Auth Only mode
Virtual Published Apps / RDSH (on-prem)	Yes		Yes	Auth Only Mode
Virtual Desktops (Cloud)	Yes		Yes	Auth Only Mode
Virtual Published Apps / RDSH (Cloud)	Yes		Yes	Auth Only Mode

Imprivata Fast User Switching (FUS) Workflows	Imprivata Windows Agent	Imprivata PIE Agent	IGEL Agent for Imprivata	Notes - IAFI
Citrix - Epic Only	Yes	Yes	Yes	Follow Policies Mode
Citrix – Virtual Kiosk	Yes	Yes	Yes	Follow Policies Mode
Citrix – Persistent App	Yes	Yes	No	

Appendix C: IGEL OS Supported Version Release Note Excerpts

- 11.08.440 - New Features 11.08.440 (igel.com)
  - General Availability of IGEL Agent for Imprivata.
  - This requires a WE add-on license.
- 11.09.100 - New Features 11.09.100 (igel.com)
  - Added: Computer policy affects showing shutdown and reboot buttons at lock screen.
  - Added: Query email from standard principal information. The following registry key will override it with an email provided by the App Moniker - if available.

Parameter	**Query Email from App Moniker**
Registry	query_moniker
Range	boolean
Value	**enabled** / disabled

  - Added: Reporting IGEL OS version to Imprivata Appliance
  - Added: Display username on 2nd factor query
  - Added: Minor UI improvements
- 11.09.150 – New Feature 11.09.150 (igel.com)

IGEL Agent for Imprivata

Experimental Features – Follow Policies Mode:

- **Added:** In FUS and Follow Policies mode, only Citrix sessions being started by the IGEL Agent for Imprivata will be disconnected / signed out, others remain intact.
- **Added:** the resource chooser is now part of the lock screen (if lock screen is enabled).
- Changed chooser from a grid view to list view
- **Added:** registry key for hiding horizon apps on chooser (and thus show desktops only)
- NOTE: With the setting enabled, if the user only has one desktop assigned, it will launch the desktop (honors Imprivata VDA policy setting).

Parameter	**Hide Apps from the Horizon Chooser**
Registry	hide_horizon_apps_on_chooser
Range	boolean
Value	**enabled** (default) / disabled

KNOWN ISSUE:

- With the **hide_horizon_apps_on_chooser** setting enabled, the App filter engages too quickly and you will see an error message: "Entitlement Not Found"
  - **Resolution:** disable this setting
  - **Result:** if the user has more than one Horizon desktop resource, the chooser will show both desktops and apps (no filter applied)
  - This will be fixed in an upcoming agent release

- Added reg key for hiding Citrix apps on chooser (and thus show desktops only)

Parameter	**Hide Apps from the Citrix Chooser**
Registry	hide_citrix_apps_on_chooser

Range	Boolean
Value	**enabled** (default) / disabled

- Added the ability to run Horizon Apps
- Changed reg key 'query_moniker' from bool to string to hold the moniker name to query for from the appliance.

Parameter	**Query Email from this App Moniker**
Registry	query_moniker
Range	String
Value	enabled / **disabled** (default)

- Fixed: Program rfideas also in FUS mode
- Fixed: Password change

Appendix D: IGEL Agent for Imprivata Registry Settings

OS 11 Menu Path: System → Registry → iia

Parameter	UMS Setup UI: Accessories – IGEL Agent for Imprivata	Options	Description/Notes	IAFI Workflow	
				Auth Only	Follow Imprivata Policies
allow_tapover	Yes	**enable (default)**; disable	Allow user switching via badge tap. Previous session will be disconnected or logged off	Yes	Yes
auth_only_session	Yes	**Blank field – available when Follow Policies mode is disabled**	Specify the name of the Preconfigured Session in this field	Yes	N/A
bgimage	No	**default** appliance manual edit	Related to the **lockscreen** setting but can also be used with the compact logon screen. **Default** is an IGEL background. **Appliance** uses the Imprivata Computer Policy Customization setting. **Manual Edit** you can put an image file into the /wfs/ directory (ex: wallpaper.jpg)	Optional	Optional
connection_timeout	No	**Default is 5 seconds.** This can be adjusted to a higher or lower timeout value in seconds.	Appliance failover connection timeout.	Yes	Yes
default_domain	No	Blank field	Type the default Imprivata domain if there are multiple on the appliance	Yes	Yes
enabled	Yes	enable / **disable (default)**	Activate the agent by enabling this option. Requires the appliance certificates to be in the **/wfs/ca-certs** directory.	Yes	Yes
exit_default authonly followvdi	No	**logoff / disconnect** authonly: logoff followvdi: disconnect	Default for how to leave auth only or follow vdi sessions on Tap Out or Tap Over.	Yes	Yes

follow_policies	Yes	**enable (default)** / disable	When enabled, this setting disables the Auth Only workflow option.	N/A	Yes
fus	No		Imprivata FUS - Citrix only ** requires Follow Imprivata Policies setting and Computer Policy FUS setup	N/A	Yes
crypt_password	No	manual edit	FUS user's password	N/A	Yes
domain	No	manual edit (should be FQDN)	FUS user's domain	N/A	Yes
resource	No	manual edit	FUS user's resource (ex: name of Citrix published app/desktop)	N/A	Yes
fus_store	No	manual edit	Citrix Storeweb URL (requires HTTP Basic to be enabled. Same as for PIE Agent)	N/A	Yes
user	No	**manual edit** / Hostname / MAC address / Serial of the board	User ID for the FUS resource being launched.	N/A	Yes
hide_citrix_apps_on_chooser (Experimental Feature)	No	**enable (default)** / disable	Filters out Citrix app icons on a chooser and only shows desktop resources if there are multiple. Best used with the **lockscreen** feature.	N/A	Yes
hide_horizon_apps_on_chooser (Experimental Feature)	No	**enable (default)**/ disable	Filters out Horizon app icons on a chooser and only shows desktop resources if there are multiple. Best used with the **lockscreen** feature.	N/A	Yes
hide_on_idle	No	enable / **disable (default)**	Minimizes the agent dialog after authenticating the user.	Optional	Optional
ignore_readers	No	manual edit (A list of pcsc readers that will display as an attached proximity reader and will be ignored. Multiple entries can be used separated by a semicolon.)	As needed - usually required for IGEL UD3/UD7 devices with an embedded PCSC reader (HID Omnikey) or for a keyboard with a PCSC reader built in like a Cherry keyboard.	Yes	Yes

launch_sole_horizon_desktop	No	**enable (default)** / disable	Similar to PIE, if a user only has one Horizon desktop, launch with no prompt/chooser	N/A	Yes
lockscreen	No	enable / **disable (default)** When disabled, the agent will start in compact mode (bottom right corner of the IGEL desktop).	Full Screen Lock/Logon. Background image can be customized - refer to **bgimage** setting. NOTE: you can use a hotkey to toggle between the full lock screen and compact screen. The hotkey combination is: “ESC + I”	Yes	Yes
log_level	No	error / **info (default)** / debug	Logging verbosity. Debug should only be used for short term troubleshooting. Return to info for normal production use.	Yes	Yes
noverify	No	enable / **disable (default)**	Skip appliance certificate validation. For troubleshooting only.	Yes	Yes
path_to_certificate	**Yes**	**default is /wfs/ca-certs/**	From UMS, deploy the certs as files - Common Certificate or SSL certificate. You don’t have to specify the name of the exact certificate. Just leave the default setting as is.	Yes	Yes
preselect_resource citrix horizon microsoft	Yes	manual edit		N/A	Yes
query_moniker	No	manual edit	Query email from App Moniker (will override user's default email). This is used for AVD / W365 Cloud PC support. We pull the UPN/email using the appliance Web API.	Yes	N/A

Rfideas format write_rfideas_cfg	No				
server	Yes	Enter the URL to the Server(s). Multiple appliances can be listed separated by a semicolon and no spaces.	Must use the appliance(s) FQDN ex: https://appliance.imprivata.org	Yes	Yes
stuff_cred	Yes			Yes	N/A
try_kerberos	No	Enable / disable	Experimental feature		
vc avd citrix horizon rdp	No				

Appendix E: Error Messages

Insert table of messages with info on what it means, etc