



Privileged Access Management
for Small and Medium-Sized Businesses

User Manual

2020.2

Table of Contents

Part I Overview	9
1 What is Devolutions Server?	10
2 System Requirements.....	12
3 Topologies	14
4 Fault Tolerance.....	19
Part II Getting Started	21
1 Security Checklist.....	23
LDAP over SSL	24
Encrypting Connections to SQL Server	25
2 Team Edition	25
Part III Installation	27
1 Installing Web Roles Prerequisites.....	29
2 Database Instance.....	34
On-Premise	34
Microsoft Azure SQL	34
3 Create Devolutions Server instance.....	35
4 Upgrading Devolutions Server.....	50
Part IV Management	57
1 Devolutions Password Server Console.....	58
Devolutions Server Settings	59
General.....	59
Database	61
Advanced Settings.....	64
Authentication	66
Domain	68
Office365	72
IIS	75
Advanced.....	77
Commands	78
Import Users.....	80
Backup Manager.....	81
Database	82
Advanced	85
View logs.....	87
Explore content of website directory.....	88
Pack Data Source.....	88
Options.....	91
Advanced	92
Check Prerequisites.....	93

	Database Diagnostic.....	95
	Send Diagnostic to Support.....	96
	View Installation Logs.....	99
	Open Backup Folder.....	100
	Manage Encryption Keys.....	102
	Check for Updates.....	104
	About.....	105
2	Authentication.....	107
3	Security	109
	User Management	110
	Role Management	120
	Legacy properties.....	126
	Vault Management	128
	Part V Web Interface.....	135
1	Dashboard	137
2	Account Menu.....	138
3	Vaults	146
	My Vault (Private)	149
	Create a New Entry	150
	Session.....	153
	RDP (Microsoft Remote Desktop).....	153
	Apple Remote Desktop (ARD).....	171
	Information.....	176
	Alarm Codes.....	177
	Email Account.....	179
	Website	186
	Note/Secure Note.....	188
	Contact.....	189
	Document.....	191
	Folder	194
	Credential Entry.....	196
	Connection String.....	197
	One-Time Password (OTP).....	199
	Password List.....	201
	Private Key.....	203
	Username/Password.....	205
	Import.....	207
4	Reports	211
	Configuration	215
	Scheduling Reports	215
	Diagnostic.....	219
5	Administration.....	221
	Security Management	223
	Users.....	223
	General	224
	Information.....	226
	Two Factor.....	227
	Roles	228
	Applications.....	229
	Vaults	230

Settings	231
Applications.....	232
Vaults.....	233
Users Locked.....	234
Users 2FA Status.....	235
Reset Server Cache.....	236
Notifications.....	237
Subscribers.....	239
Subscriber Groups.....	242
Subscriptions	243
Configuration	245
System Settings.....	245
General	246
System Message.....	249
Password Policy.....	249
Password Template.....	251
Forbidden Password.....	252
Type Availability.....	253
User Template.....	254
Advanced.....	255
Password Server Settings.....	256
General	257
General	257
Authentication.....	259
Domain	261
Office365.....	265
Email	268
Logging	270
Features	273
Scheduler.....	274
Advanced.....	275
Security	276
Two-Factor.....	276
SMS	280
Backup Codes.....	281
Security	285
GeoIP Security.....	287
Privileged Access Management.....	289
System Permissions.....	291
Entries	292
Management.....	293
Miscellaneous.....	295
Tools	296
Privileged Access Management.....	297
Templates	298
Password Templates.....	298
Templates.....	301
Backup	301
Backup Manager.....	301
Backup List.....	304
Logs	306
Cleanup Logs.....	306
Advanced configuration.....	308
6 Role Based Security.....	310

Permissions	320
-------------------	-----

Part VI Privileged Access Management 329

1 Getting Started.....	331
2 Accounts	338
3 Providers	340
Domain Provider	342
Local SSH Provider	344
SQL Server Provider	346
4 Scan Configurations.....	348
Domain Account Discovery	352
SSH Account Discovery	355
SQL Account Discovery	358
5 Checkout Process.....	361
6 View Sensitive Data vs Account Brokering.....	366

Part VII Devolutions Web Login 369

1 Overview	370
2 Installation	371
Chrome	372
Firefox	373
Microsoft Edge Beta	375
Opera	379
3 First Login	380
Password Hub	380
Multiple Password Hub	384
Password Server	390
Remote Desktop Manager	393
4 Exploring Devolutions Web Login.....	395
Menu	395
Settings.....	396
Retrieve Credentials	400
Remote Desktop Manager.....	401
Secure Devolutions Web Login	402
Keyboard Shortcuts	404

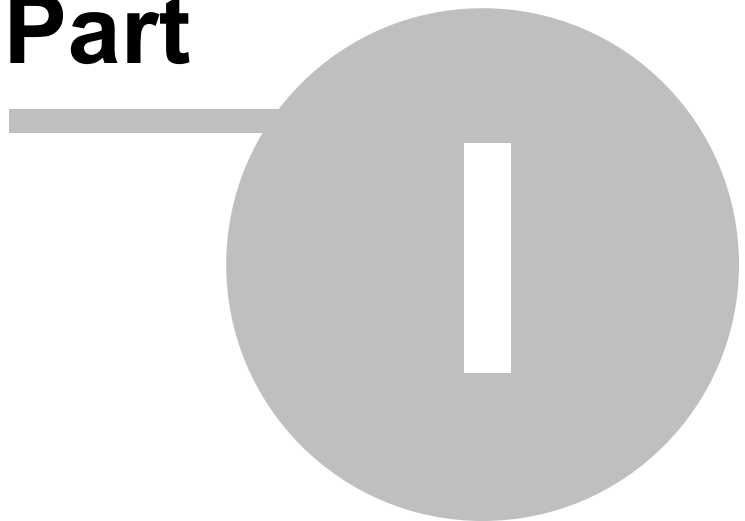
Part VIII Devolutions Launcher 407

1 Overview	408
2 Installation	409
Prerequisites	409
Windows	410
macOS	417
Android	418
iOS	419
3 Configuration and Settings.....	420
Devolutions Password Server	420
Windows.....	423
macOS.....	427

Android	432
iOS	436
Devolutions Password Hub	440
Windows	440
Android	444
iOS	448
4 Utilization	452
Windows and macOS	452
Android and iOS	454
Part IX Support/Resources	457
1 FAQ (Frequently Asked Questions).....	458
2 Previous Versions.....	460
3 Technical Support.....	460

Overview

Part



1 Overview

1.1 What is Devolutions Server?

DESCRIPTION

This documentation is valid for version 2020.2.0. [Previous Versions](#)



Devolutions Server is an **on-premise** vault for storing and **sharing** information across your whole organization. Manage remote connections, credentials, and sensitive information with ease.

Use our **Role Based Access Control** to grant permissions in a granular fashion. Advanced logging of all user activity is included to offer visibility in all aspects of the solution.

Because of its Web Architecture you have the possibility to offer it only from your intranet or publish it on the Internet.

There are two ways of using Devolutions Server:




Web-Based Vault



Session Management

Web browser access and Devolutions Web Login	Using a client application (desktop or mobile)
<p>Access vaulted resources from a web browser using a Client Access License (CAL). Credentials are managed directly from the web interface and no client application is required.</p> <p>With the Devolutions Web Login browser extension, credentials can be automatically submitted when connecting to a website.</p>	<p>Access vaulted resources using our client applications which communicate with Devolutions Server web services. A local installation of a client application such as Remote Desktop Manager is required to manage the data source and its resources. Note that we offer Windows, macOS, Android and iOS editions.</p> <p>Use any type of entry, manage all aspects of the data source and monitor user activity all in the same application.</p>
<p>Remote access technologies (RDP, VNC, etc) are not supported within a web browser.</p>	<p>Unlike with web browser access, Remote Desktop Manager can launch sessions using remote access technologies.</p>

HIGHLIGHTS

 <p>HIGH-END SERVER</p>	 <p>FULL ACTIVE DIRECTORY (AD) INTEGRATION</p>	 <p>WEB ARCHITECTURE</p>
---	--	--

Installed **on-premise** on an application server.
Store entries in an unlimited number of vaults and manage access to these entries with our **Role Based Access Control**.

Users accessing the system will be granted permissions based on their membership in specific AD groups, making user management almost seamless for organizations that use AD to manage teams.

Implemented using a Web architecture so it can be exposed publicly on the **Internet** or only to your **Intranet** or **private cloud**.



TWO-FACTOR AUTHENTICATION

Widest choice of [Two-factor authentication](#) (2FA) providers. Many providers can be enabled concurrently. They can selectively be enforced per user.



EMAIL NOTIFICATIONS

Optionally receive email notifications for various events on sessions, users, roles, etc.



IP RESTRICTIONS

Controlling access to Devolutions Server from IP addresses / ranges, including GeoIP restriction and IP whitelisting / blacklisting.

1.2 System Requirements

MINIMUM REQUIREMENTS



Devolutions Server needs Microsoft .NET Framework 4.7.2 to function. Please adapt your environment depending on which version you are running.

DEPENDENCIES

- Microsoft SQL Server 2012/2014/2016/[2017/2019](#) (including Express editions).
- Azure SQL database is supported with SQL login accounts only. Azure Active Directory accounts are not supported.
- Windows 10, Windows Server 2012R2, 2016 and 2019.
- Windows Server 2012R2 domain functional level or higher.
- Microsoft .NET Framework 4.7.2 (Please refer to the [requirements for the .Net Framework](#) for operating systems).
- Internet Information Services (IIS) 7.0 or better.
- Devolutions Password Server Console must be installed on the server to manage the Devolutions Server instance(s).

SERVER SIZING

Many customers often ask how to properly customize their servers for various topologies. This is essentially unreliable because the way the system is used has a significant impact on the resource usage of each node within the chosen [Topology](#).

The great majority of setups that we have observed work well with nodes of 4GB RAM and a dual CPU. Most of these are virtualized environments, so granting more resources is relatively simple.

For a proper estimate, the following aspects must be considered:

- Number of entries stored in your instance (server details, credentials, etc.).
- Churn of these entries; do you create entries daily or are they quite static?

- Number of concurrent users that connect to the Devolutions Server instance during peak times.
- Usage of information by the users. Are they launching 10 sessions at a time, doing a batch operation that takes a few minutes and then repeating the cycle, or are they opening only a few sessions but working within them all day long. This results in **write** operations to our logs, therefore the former case is more intensive than the latter.

64-BIT SUPPORT

Devolutions Server is compatible with all 64-bit versions of Windows.

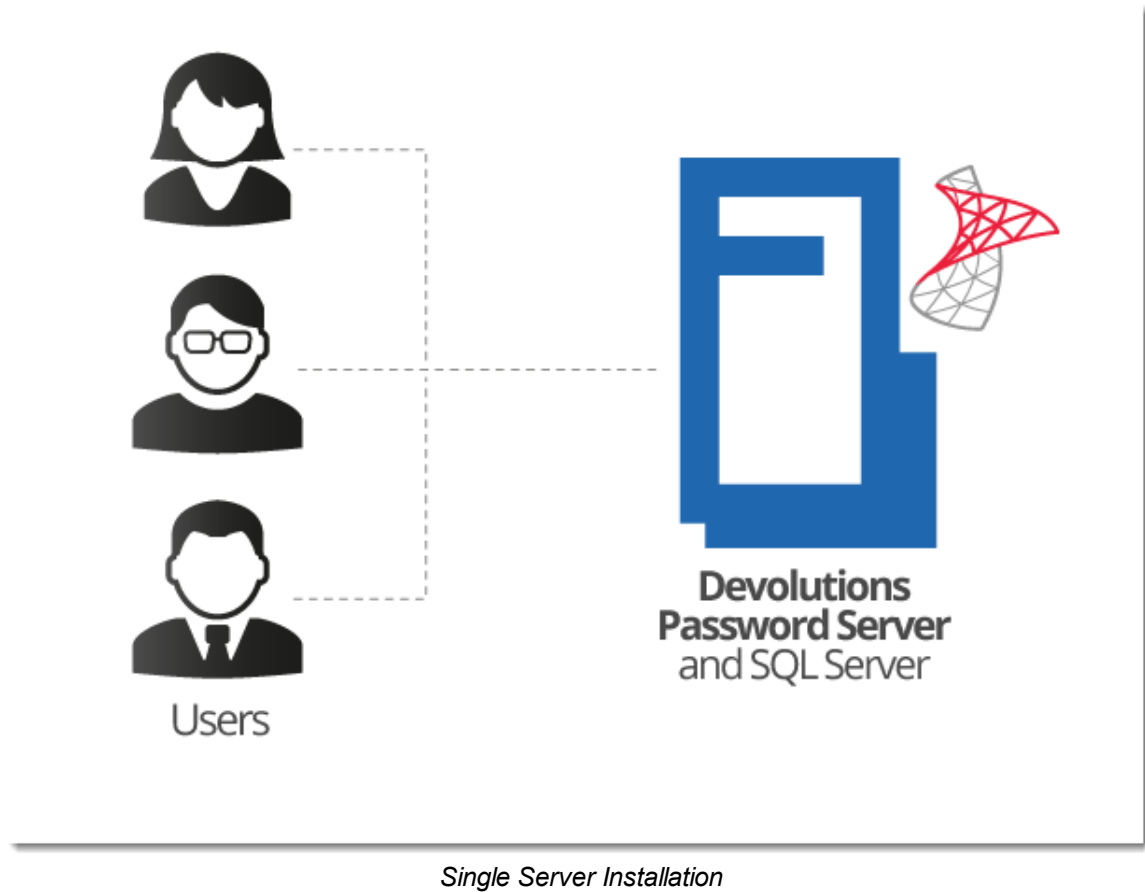
1.3 Topologies

DESCRIPTION

Devolutions Server instances can be installed through different topologies. The following are examples of different topologies serving various purposes.

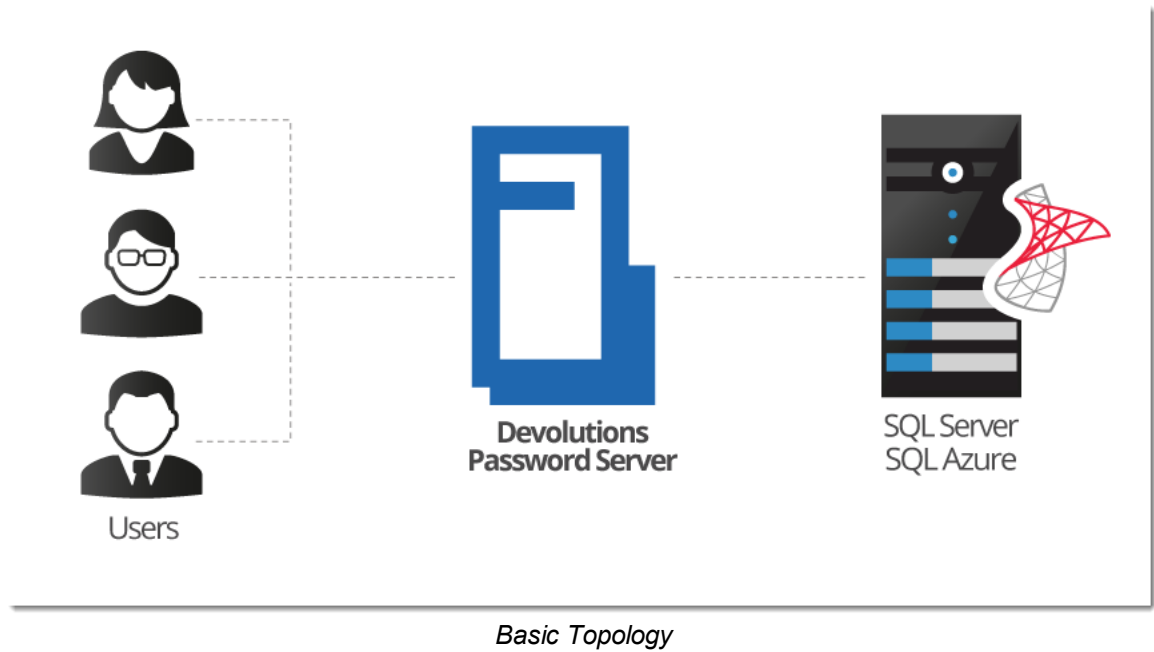
SINGLE SERVER TOPOLOGY

The Devolutions Server and the SQL Server can be installed on the same machine for a small team up to 20 users. Having Devolutions Server and SQL Server on the same machine could result in certain performance issues if you attempt to serve more than 20 users.



RECOMMENDED BASIC TOPOLOGY

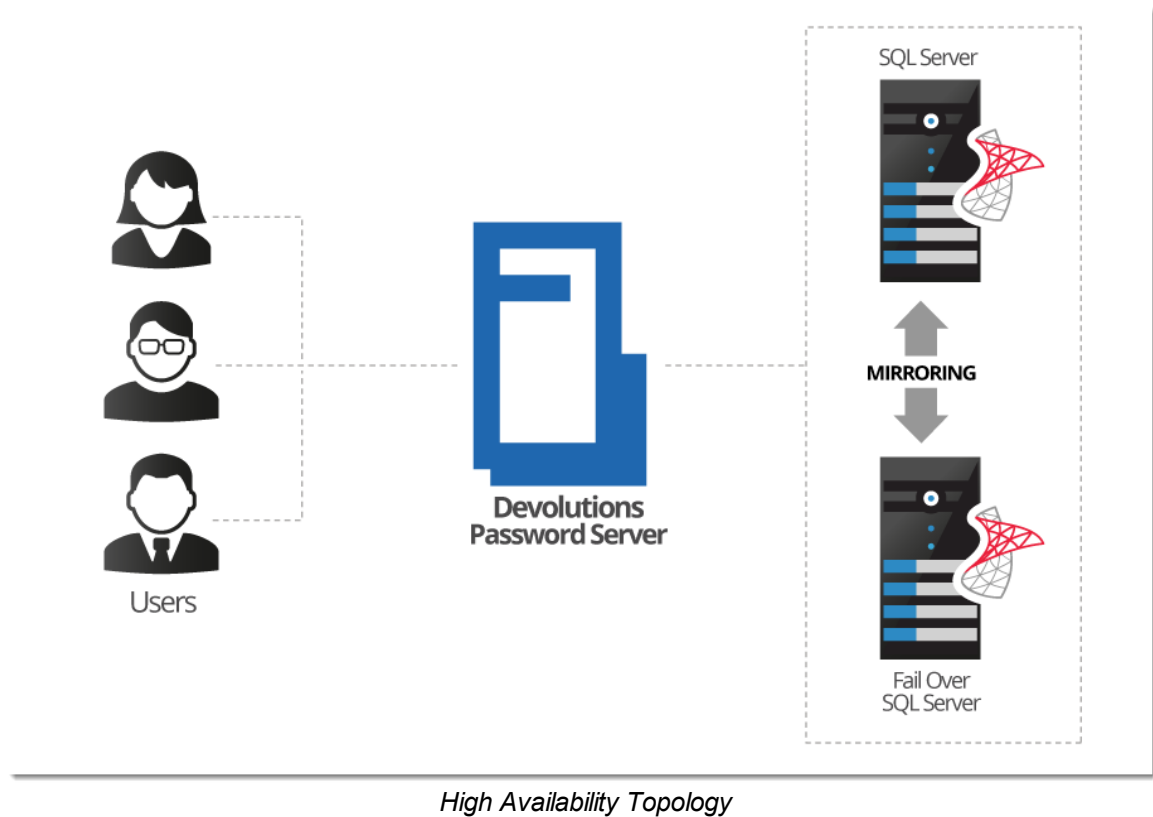
A recommended basic topology consists of two servers, one for the Devolutions Server and one for the SQL Database. By doing so, all queries are made by the SQL server and performance is less affected on the application server.



HIGH AVAILABILITY TOPOLOGY

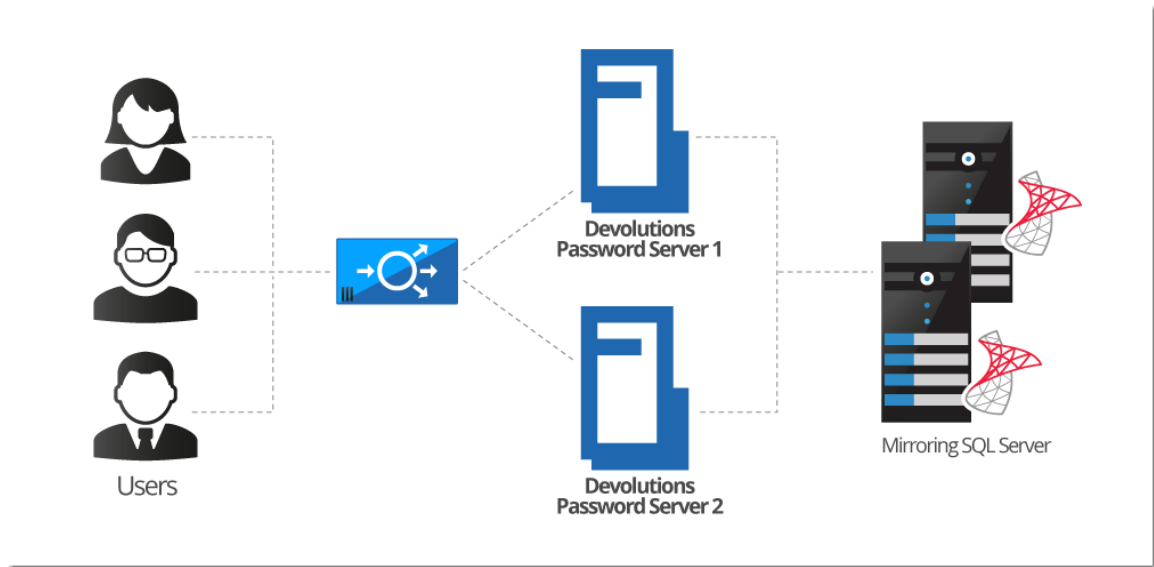
DATABASE LAYER ONLY

For a high availability of the database, Database Mirroring can be used which replicates data to a partner server. The failover partner server will be ready at anytime when the main server becomes unavailable. This ensures that the Devolutions Server is still accessing the data source and is transparent for Remote Desktop Manager users.



LOAD BALANCING TOPOLOGY

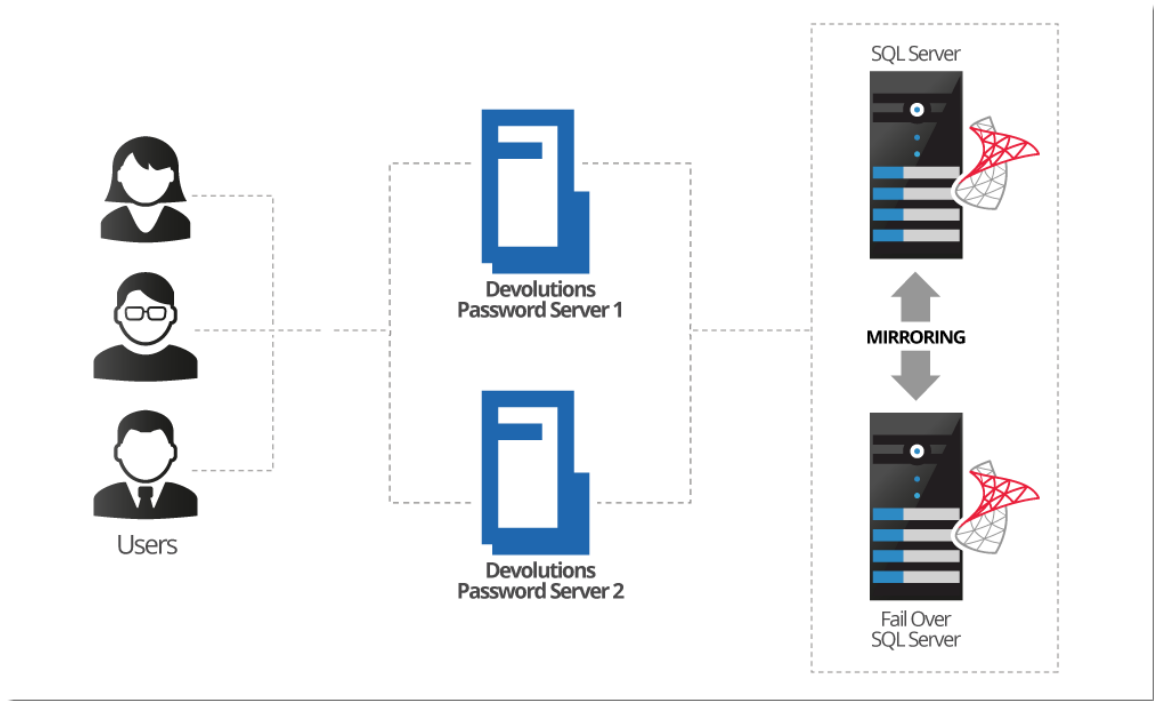
To ensure maximum performance of the Devolutions Server, it can be deployed as a load balancing Devolutions Server topology as illustrated in the image below. It can either be a physical or software load balancing system.



Load Balancing Devolutions Server Topology

DEVOLUTIONS SERVER INSTANCE MANUAL FAILOVER

For customers that do not wish to purchase a load balancer or are seeking a more simplified topology for their system, you can simply utilize two Devolutions Server instances on two different web servers and direct them to the same SQL Server database. By registering both instances as separate data sources in the client applications, users can manually toggle between servers in the scenario that one becomes unresponsive.



Manual Failover with Two Devolutions Servers

1.4 Fault Tolerance

DESCRIPTION

The Devolutions platform follows certain design guidelines to preserve full version history of your data, be it modifications or deletions. It also has an extensive logging layer to provide full visibility on the activity carried out while using the system. These design choices impact the choices offered to you when you wish to provide fault tolerance at the database level.

IMPACT ON TECHNOLOGICAL CHOICES

Because of all of the write operations that occur behind the scenes, you cannot have a topology other than ACTIVE/PASSIVE. The standby replica must be kept in sync at all times, but left untouched. There can be only ONE database in use at any one time. You can use both Microsoft technologies of mirroring or clustering, but it is key is that the replicated content is only accessed when the master content is unavailable.

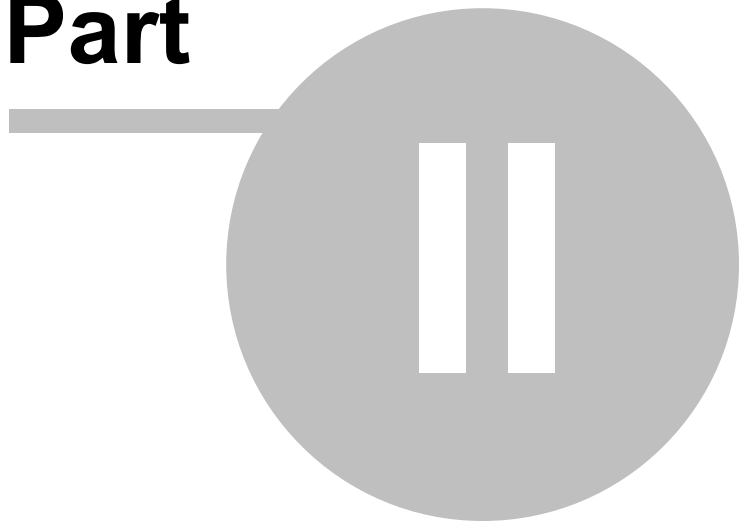
MIRRORING AS A WAY TO SHARE WITH DISTANT TEAMS

The consequence of keeping replicated data untouched means that replication is NOT the proper solution to use whenever you have multiple teams and you wish to share a set of master data across them. For this scenario it is best to use a mix of:

- [Synchronizers](#), particularly the one for RDM data.
- PowerShell scripting (to export a specific branch of your tree).

Getting Started

Part



2 Getting Started

DESCRIPTION



This topic is for **Devolutions Password Server - Corporate Edition**. If you have purchased **Devolutions Password Server - Team Edition** instead, please consult [Getting Started - Team Edition](#).

After completing your purchase of Devolutions Password Server - Corporate Edition, you will receive an email with **three** license serials. Each license serial allows for running a Devolutions Server instance. An instance is in itself a web server application which acts as a back-end for our client applications. You can think of it as a specialized database for your data. All instances can be installed on the same physical server or spread across many.

Devolutions Server can be installed through different [topologies](#).

DOMAIN REQUIREMENTS

These requirements apply especially if you intend to use Automatic User Account Creation (see [Authentication](#)) and/or [Roles](#) to manage your instance.

✓	Create Active Directory groups to manage your instance. Typical examples are: RDM Admins , RDM Operators , RDM Users .
✓	Add domain users to the Active Directory groups.
✓	Create a VaultOwner account that will be the owner of the database. Performing upgrades with this account will ensure the proper rights are held.
✓	Create a VaultRunner account that will be used as the identity of the website. This will allow you to harden the permissions to what is minimally required.

CHECKLIST FOR INSTALLING AND RUNNING DEVOLUTIONS SERVER

SOFTWARE REQUIREMENTS ON THE SERVER HOSTING THE INSTANCE

✓	Microsoft .NET Framework 4.7.2 (can be installed using the Microsoft Web Platform Installer).
✓	Microsoft SQL Server (see Database Instance) if you intend to host the solution on a single server (see Topologies).
✓	Internet Information Services (IIS) 7.0 or better (see https://technet.microsoft.com/en-ca/library/hh831475.aspx#InstallIIS).

INSTALLATION STEPS

✓	Create a new instance of Devolutions Server (see Create Devolutions Server instance).
✓	Create a Devolutions Server administrator account in the User Management .
✓	Create roles (see Role Management).
✓	Add domain users or built-in users (see User Management).

2.1 Security Checklist

DESCRIPTION

To achieve the highest level of security, you should adhere to the following guidelines.



These recommendations are valid ONLY if the Devolutions Server instance is hosted on an **intranet** EXCLUSIVELY. You must involve a person with knowledge of Internet security to safely host any application on the Internet. You need to protect the site from **Denial of Service** attacks using an appliance or a security module that is external to Devolutions Server.

GENERAL

- Use Windows Authentication exclusively.
- Ensure all LDAP communication uses [LDAP over SSL](#).

SQL SERVER

- Enable only the **Windows Authentication Mode**.
- Create a domain account that will be used to create the database (**VaultOwner**), as well as another account that will be used by the web server to connect to the database (**VaultRunner**). The latter must have only the minimal set of permissions to perform its tasks.
- Communicate **ONLY** through an encrypted connection, please see [Encrypting Connections to SQL Server](#).

WEB SERVER

- Configure the application pool to use domain credentials. This account will be added to the SQL Server as a login and be granted only the permissions that are needed (**VaultRunner**).
- Serve content through SSL (https). See [Configure SSL](#).

2.1.1 LDAP over SSL

DESCRIPTION

The LDAP over SSL (LDAPS) is a method to secure LDAP communications.

By default, LDAP communications between client and server are not encrypted. In some organizations, this could lead to a security breach.

Follow this link for further information

<http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>.

2.1.2 Encrypting Connections to SQL Server

DESCRIPTION

To ensure that the communication between the Devolutions Server instance and the SQL Server database is encrypted, an extensive procedure must be followed on the SQL Server instance.

Please consult this technet article that provides detailed instructions [Encrypting Connections to SQL Server \(technet\)](#).

After proper configuration, the only modification required in Devolutions Server is to enable the **Use SQL Server encrypted connection** in the [Database](#) tab of the instance settings.

2.2 Team Edition

DESCRIPTION

After the purchase of the **Devolutions Password Server - Team Edition**, an email is sent with the license serial. This key allows you to create a new instance of Devolutions Server.

The installation procedure is available at [Devolutions Server Installation](#)



Please check your junk/spam mail folder if you do not see the email in your inbox.

DOMAIN REQUIREMENTS

These requirements apply only if you intend to use Automatic User Account Creation (see [Authentication](#)) and/or [Roles](#) to manage your instance.

✓	Create Active Directory groups to manage your instance. Typical examples are: RDM Admins , RDM Operators , RDM Users .
✓	Add domain users to the Active Directory groups.

CHECK LIST FOR INSTALLING AND RUNNING <%TITLEBE%>

SOFTWARE REQUIREMENTS ON THE SERVER HOSTING THE INSTANCE

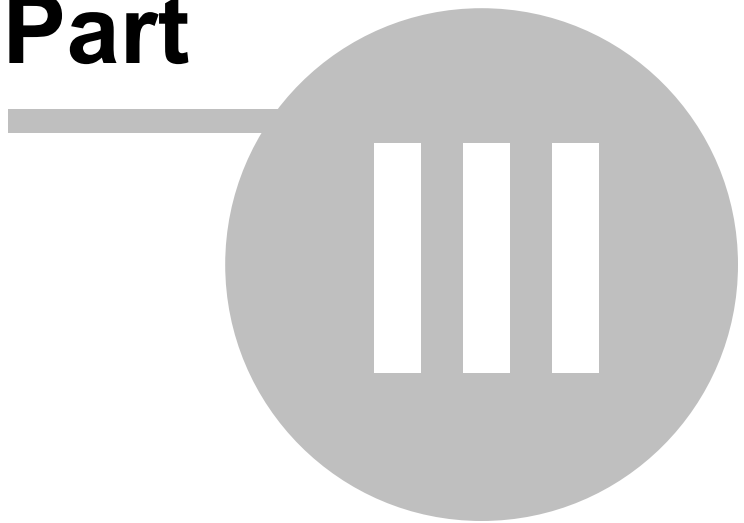
✓	Microsoft .NET Framework 4.7.2 (It can be installed through the Microsoft Web Platform Installer).
✓	Microsoft SQL Server database (see Database Instance).
✓	Information Services (IIS) 7.0 or better (see https://technet.microsoft.com/en-ca/library/hh831475.aspx#InstallIIS).

INSTALLATION STEPS

✓	Create a new instance of Devolutions Server (see Create Devolutions Server Instance).
✓	Create a Devolutions Server administrator account in the User Management .
✓	Create Roles (see Role Management).
✓	Add domain users or built-in users (see User Management).

Installation

Part



3 Installation

TOPOLOGY



If you just have received your license serials, please refer to the [Getting Started](#) topic.

A Devolutions Server instance is actually a web application. This allows for exposing its services on the Internet or an Intranet.

The recommended [topology](#) is the use of two servers: a Database server and a Web server. For smaller installations, a single server can be used, but resources will be shared between the two roles, thereby minimizing performance.



The Devolutions Password Server Console is now offered as a stand alone application. It is available on the [Download page](#).



Please ensure before starting the installation that you have **.NET 4.7.2** installed on your machine. You can download it on the following page. <https://dotnet.microsoft.com/download/dotnet-framework-runtime/net472>



It's highly recommended to enable SSL Encryption in order to protect communication with the instance of the SQL Server. Please follow the instructions on <http://support.microsoft.com/kb/316898>. Note that we recommend this be done **after** the initial setup is complete.



For full Active Directory integration, the application pool uses a domain identity. Both servers need to be joined to the domain.

INSTALL DEVOLUTIONS SERVER

WEB SERVER PREREQUISITES

Please refer to the appropriate topic depending on the operating system of the web server.

INSTALLING WEB ROLES

Please refer to the [Installing Web Roles Prerequisites](#) topic.



After you have installed the pre-requisites, test the IIS installation by navigating to <http://localhost>. **Do not proceed further** if you do not see the IIS welcome screen. There are issues that must be resolved.

DATABASE SERVER PRE-REQUISITES

Please refer to the [Database Instance](#) topic.

CREATE DEVOLUTIONS SERVER INSTANCE

Please refer to the [Create Devolutions Server instance](#) topic.

3.1 Installing Web Roles Prerequisites

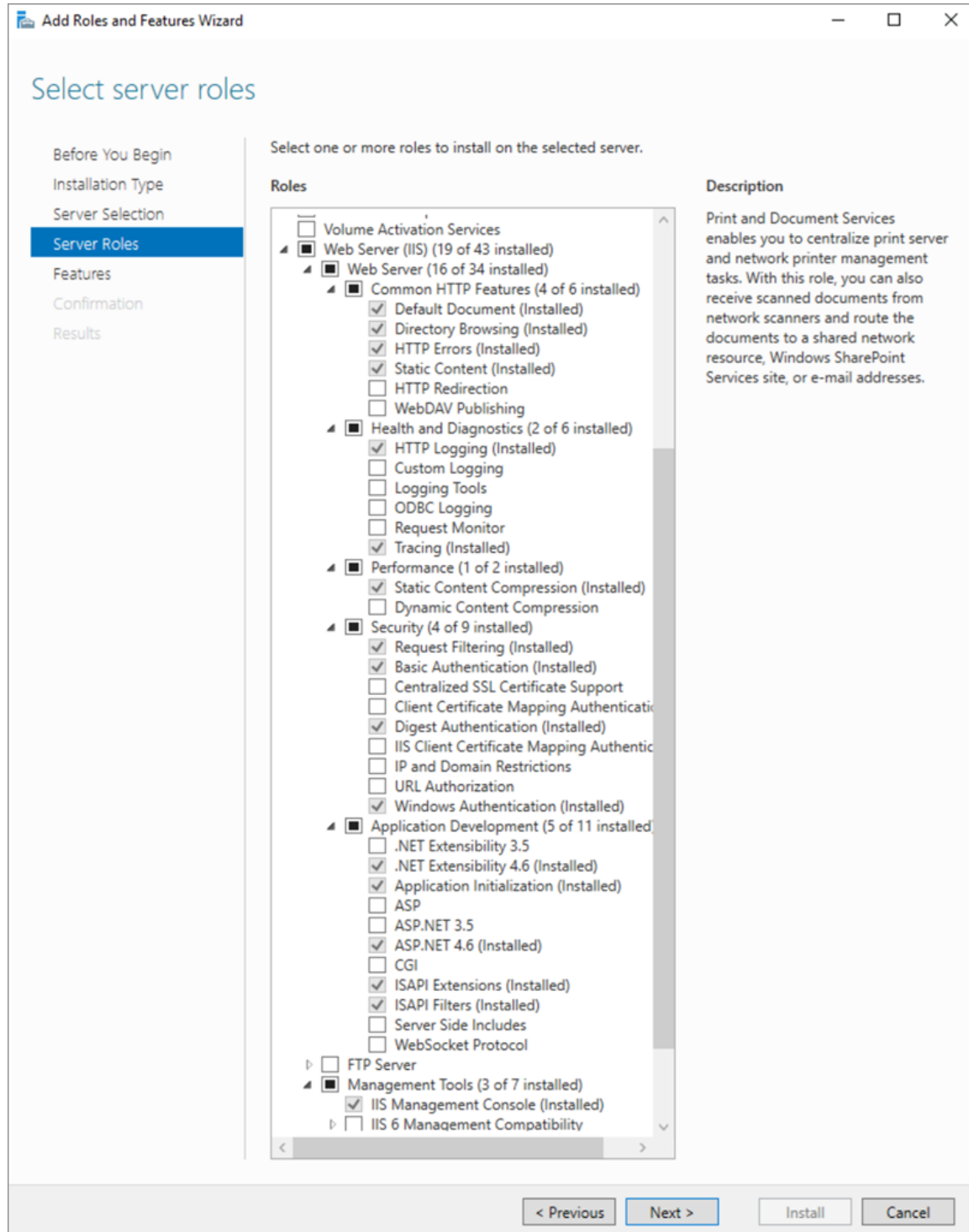
DESCRIPTION



The installation of the Devolutions Server is supported by Windows 10, Windows Server 2012R2, 2016 and 2019. For previous Windows Server versions, please consult the PDF documentation of previous Devolutions Server.

As a web application, Devolutions Server requires the IIS Manager, the URL Rewrite Module and specific Web Roles on the machine on which it will be hosted. It is possible

to install these prerequisites, IIS Manager and URL Rewrite Module included, from the Devolutions Password Server Console or through an existing PowerShell scripts provided with Remote Desktop Manager Enterprise Edition for Windows.



Web Roles needed for Devolutions Server



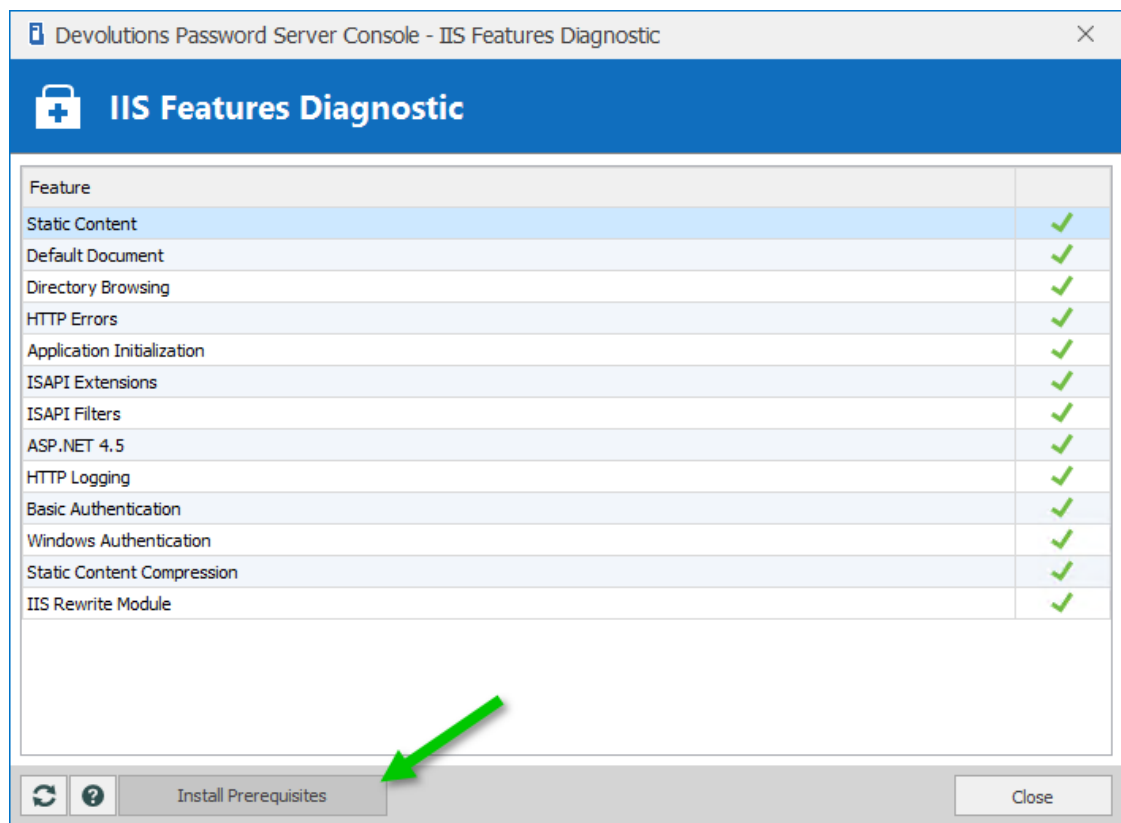
Installing prerequisites from [Devolutions Password Server Console](#) or from the PowerShell script require internet access to download [Web Platform Installer](#) and [URL Rewrite Module](#).

STEPS

Here are the two different methods available to install the prerequisites:

1. Devolutions Password Server Console

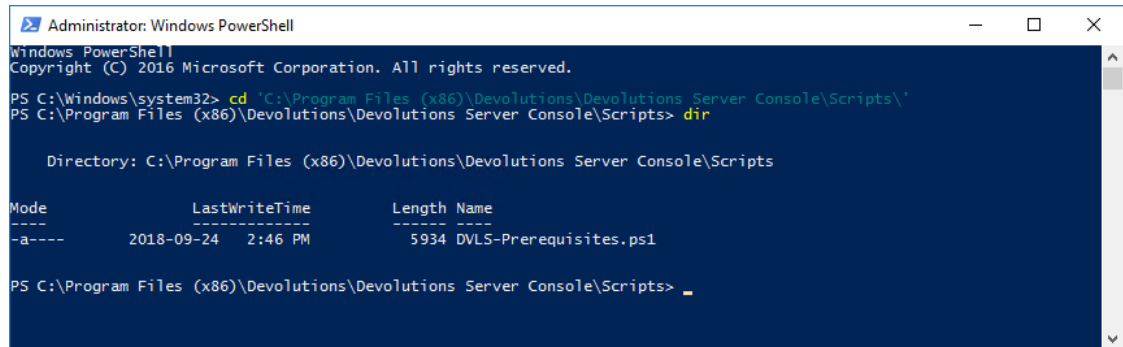
- a. Open the [Devolutions Password Server Console](#).
- b. Expand the [Advanced](#) menu and select [Check Prerequisites](#).
- c. Click on the Install Prerequisites button to run the PowerShell script.



IIS Features Diagnostic Dialog

2. PowerShell command line

- a. Run Windows PowerShell with elevated privileges.
- b. Change the current path to the sub-folder Scripts that is located in the current installation folder of Devolutions Password Server Console.
(**C:\Program Files (x86)\Devolutions\Devolutions Server Console\Scripts**)



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd 'C:\Program Files (x86)\Devolutions\Devolutions Server Console\Scripts\'
PS C:\Program Files (x86)\Devolutions\Devolutions Server Console\Scripts> dir

    Directory: C:\Program Files (x86)\Devolutions\Devolutions Server Console\Scripts

Mode                LastWriteTime         Length Name
----                -
-a-----         2018-09-24   2:46 PM           5934 DVLS-Prerequisites.ps1

PS C:\Program Files (x86)\Devolutions\Devolutions Server Console\Scripts>
  
```

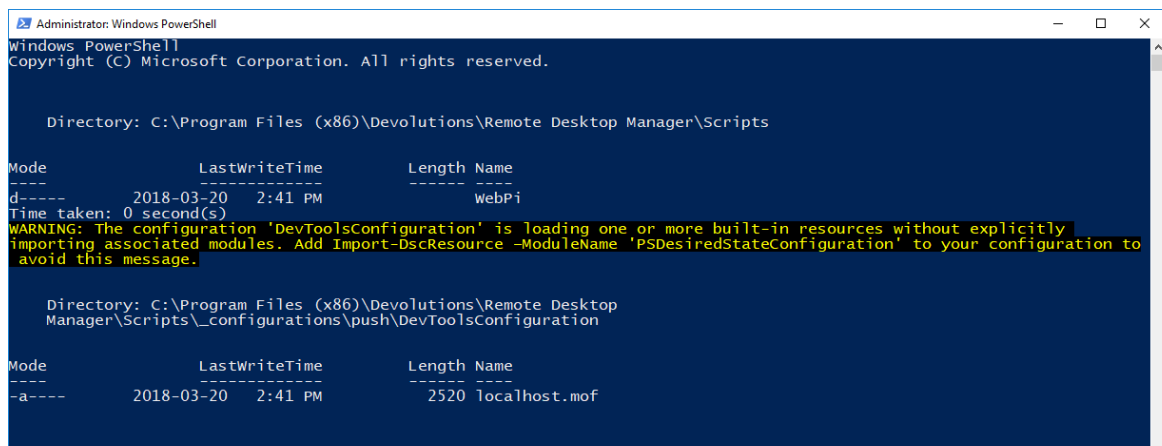
Location of DVLS-Prerequisites PowerShell script

- c. Run the script DVLS-Prerequisites.ps1.

RESULTS

Here is what the installation of these prerequisites through the PowerShell script should display.

1. On the beginning of the PowerShell script, it will install Microsoft Web Platform Installer if it is not already installed.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

    Directory: C:\Program Files (x86)\Devolutions\Remote Desktop Manager\Scripts

Mode                LastWriteTime         Length Name
----                -
d-----         2018-03-20   2:41 PM           webPi
Time taken: 0 second(s)
WARNING: The configuration 'DevToolsConfiguration' is loading one or more built-in resources without explicitly
importing associated modules. Add Import-DscResource -ModuleName 'PSDesiredStateConfiguration' to your configuration to
avoid this message.

    Directory: C:\Program Files (x86)\Devolutions\Remote Desktop
Manager\Scripts\_configurations\push\DevToolsConfiguration

Mode                LastWriteTime         Length Name
----                -
-a-----         2018-03-20   2:41 PM           2520 localhost.mof
  
```

PowerShell Window

- Next, the Command windows is displayed and will install the IIS Manager, ASP .Net 4.5, some specific Web Roles and the URL Rewrite Module.

```

C:\Program Files\Microsoft\Web Platform Installer\WebpiCmd.exe

The software that you obtain using the Web Platform Installer Command Line Tool is licensed to you by its owner. Microsoft grants you no rights for third party software.
Successfully loaded primary feed: https://go.microsoft.com/?linkid=9842185
The following software is going to be installed:
EULA: 'IIS: WAS Process Model', which is owned by 'Microsoft' will be turned on
EULA: 'IIS: WAS Configuration API', which is owned by 'Microsoft' will be turned on
EULA: '.NET 4.5 Extended with ASP.NET for Windows 8', which is owned by 'Microsoft' will be installed
The license agreement to '.NET 4.5 Extended with ASP.NET for Windows 8' may be included with the software.
You are responsible for and must separately locate, read and accept these license terms.
EULA: 'IIS: Static Content', which is owned by 'Microsoft' will be turned on
EULA: 'IIS: Management Console', which is owned by 'Microsoft' will be turned on
EULA: 'URL Rewrite 2.1', which is owned by 'Microsoft', will be downloaded from 'http://download.microsoft.com/download/D/D/E/DDE57C26-C62C-4C59-A18B-31D58B36ADA2/rewrite_amd64_en-US.msi'.
The license agreement to 'URL Rewrite 2.1' is available at 'http://download.microsoft.com/download/D/D/E/DDE57C26-C62C-4C59-A18B-31D58B36ADA2/URL%20REWRITE%20MODULE-Final-EN.rtf'.
Accepted EULA.
Starting Installation
Started installing Products...
Started downloading products...
Started installing: 'IIS: WAS Process Model'
Started downloading: 'URL Rewrite 2.1'
Downloaded: 'URL Rewrite 2.1'
..

```

IIS Installation

- Then, the PowerShell script will install all missing Web Roles.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

Preparing modules for first use.
Default status description.
00:00:00 remaining.
[ABELISLE] Test-TargetResource
Collecting data...
57%
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]

Time taken: 0 second(s)
WARNING: The configuration 'DevToolsConfiguration' is loading one or more built-in resources without explicitly
importing associated modules. Add Import-DscResource -ModuleName 'PSDesiredStateConfiguration' to your configuration to
avoid this message.

Directory: C:\Users\Administrator\desktop\_configurations\push\DevToolsConfiguration

Mode                LastWriteTime         Length Name
----                -
-a----          2018-03-19 10:34 AM             2376 localhost.mof
WARNING: [ABELISLE]: [!] A reboot is required to progress further. Please reboot the system.

```

Web Roles Installation

3.2 Database Instance

DESCRIPTION

Devolutions Server has no requirements that would dictate which communication protocol is used, as well as many of the options offered to you by the chosen SQL Server instance. As long as the client workstation can connect to the SQL instance, Devolutions Server will run effectively. Please refer to the Microsoft Documentation in order to allow connectivity to the instance.

With Windows authentication, you must set the Application Pool identity to an account from the domain. We recommend creating a dedicated account for this purpose. Please refer to [Configure Devolutions Server to use integrated security](#) for instructions that need to be performed **after** creating the Devolutions Server instance.

3.2.1 On-Premise

DESCRIPTION

Install any edition of **Microsoft SQL Server**. Many of our customers with less than 30 users run successfully with the free edition called **SQL Server Express**. [Download SQL Server 2017 Express from Microsoft's site](#).

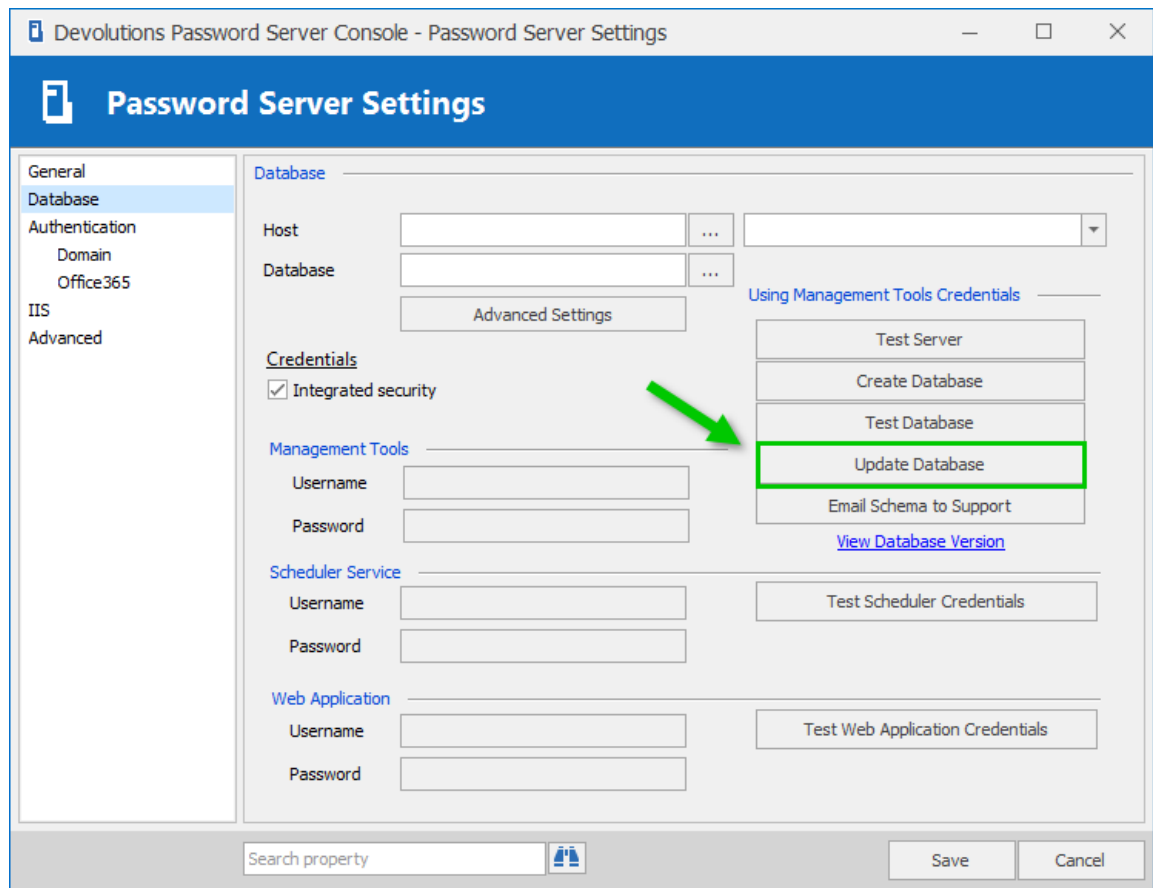
If full integration with Active Directory is required, you can decide to activate Windows Authentication solely. Please refer to the [MSDN online help](#) for full details.

3.2.2 Microsoft Azure SQL

DESCRIPTION

Create an empty SQL database on your Microsoft Azure SQL portal. Provide enough privileged to an account you will use to update the database schema from the Devolutions Password Server Console.

Once all fields are properly configured, click on the **Update database** button to update the database schema.



Devolutions Password Server Console - Database Tab

3.3 Create Devolutions Server instance

DESCRIPTION



If you have recently received your serial licenses keys, please refer to the [Getting Started](#) topic.



For more information about any of the features in the deploy wizard, please consult their respective topic under the [Server Settings](#) chapter.

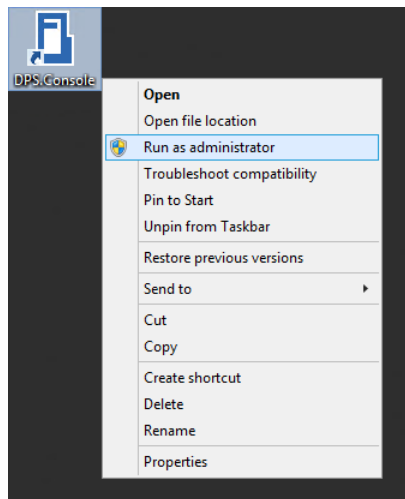
Multiple Devolutions Server instances can be hosted on the same server. Each instance resides in its own Web Application within IIS. The following steps are carried out using the **Devolutions Password Server Console**.

PROCEDURE

1. Install **Devolutions Password Server Console** on the web server. It is available from the [Download](#) page
2. Execute **Devolutions Password Server Console** with elevated privileges (run as administrator). This is performed by right-clicking on the application, and selecting **Run as administrator**.

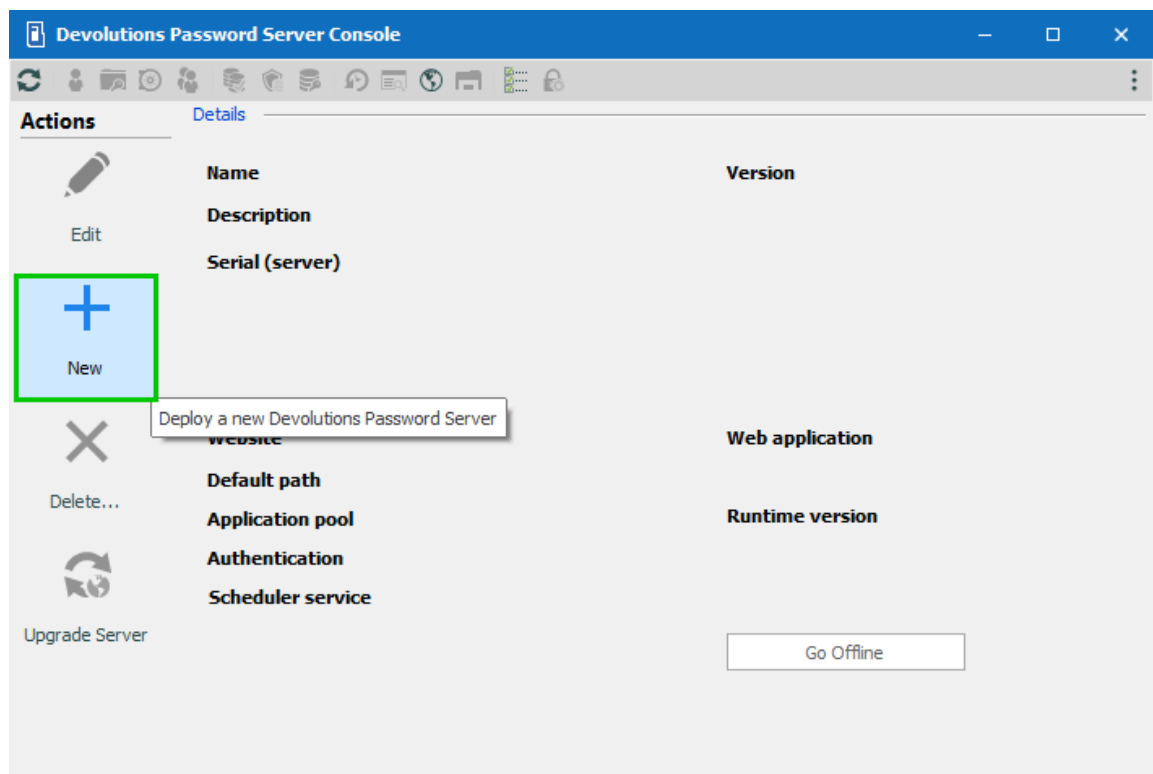


All operations performed through the console are done with the credentials used to launch **Devolutions Password Server Console**. If you must use other credentials, you will need to launch another Windows session. The RunAs command does not offer the option of starting a process with elevated privileges.




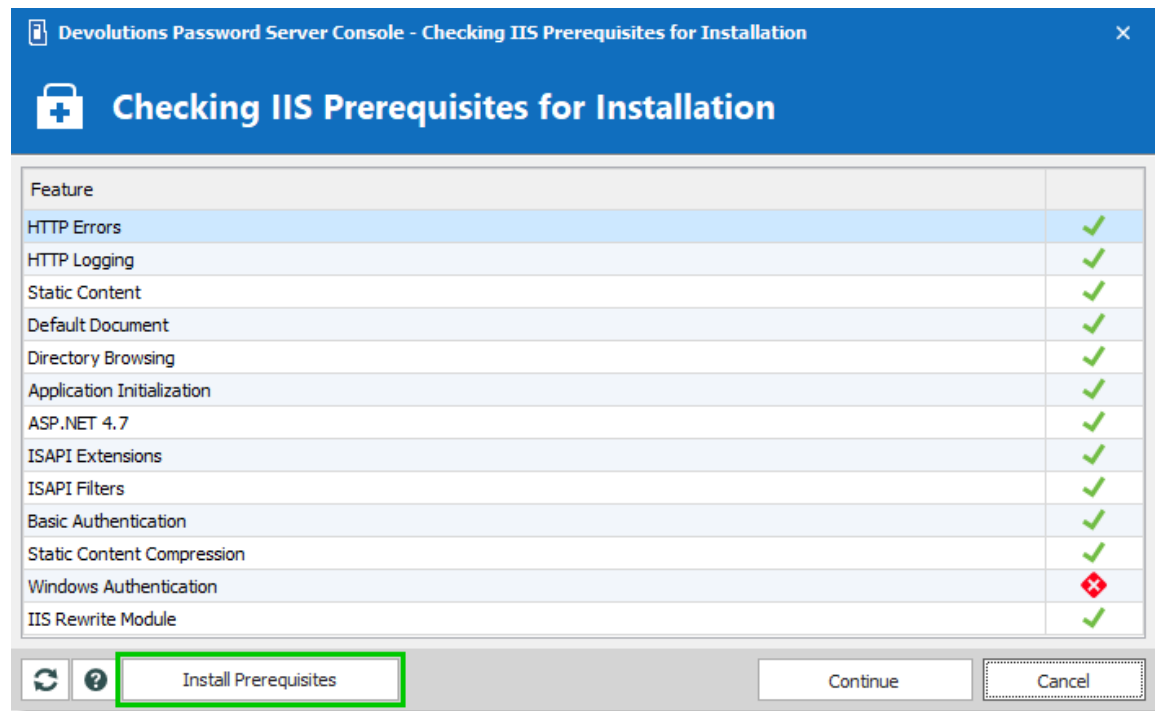
Run as administrator

3. In the **Devolutions Password Server Console**, click on the **+ New** button to deploy a new server instance.



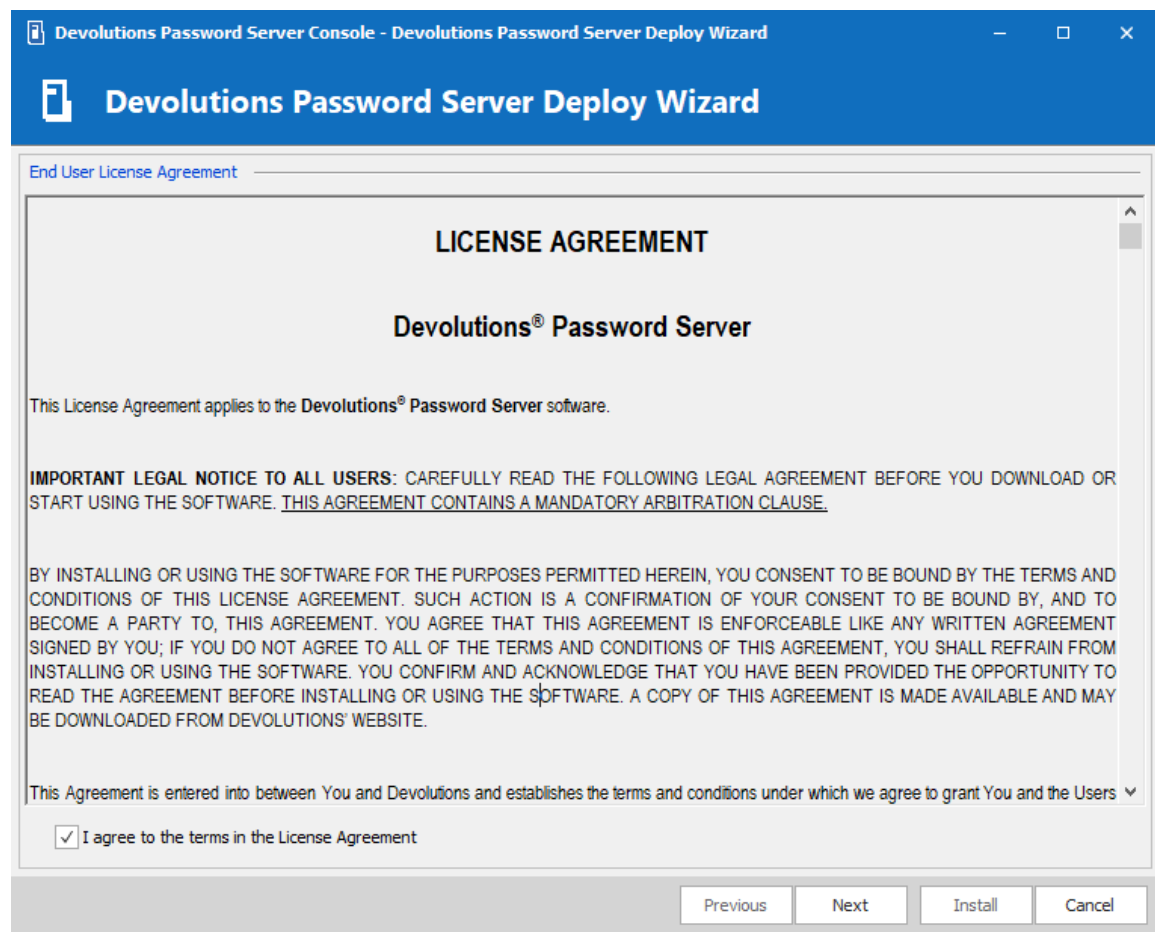
Deploy a new Devolutions Server

4. The first dialog will run diagnostics on the server to verify if the IIS Server has all the necessary Web Roles prerequisites installed and is ready to run Devolutions Server. Missing features are marked with an . The Install Prerequisites button will install all missing features using a PowerShell script.



IIS Features Diagnostic Dialog

5. The License Agreement needs to be accepted to proceed.



Devolutions Server License Agreement Dialog

6. Under **Database**, enter the server and database information, then create the database using the **Create Database** button.
The user account used to create the database must have sysadmin privileges in the SQL Server instance. Consult the [Database](#) topic for more information.
To use **Integrated Security** to connect to the database, it is important to change the Application Pool Identity in the IIS Manager and set the proper permission of the service account on the SQL database.

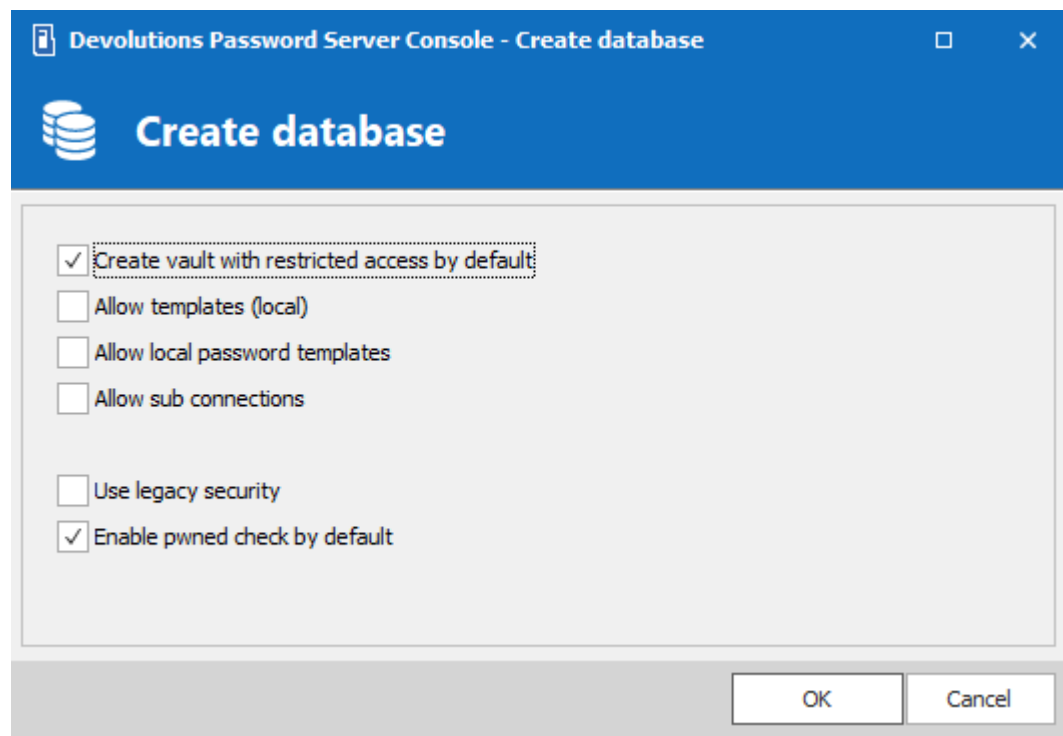
The screenshot shows the 'Database' tab of the 'Devolutions Password Server Deploy Wizard'. The window title is 'Devolutions Password Server Console - Devolutions Password Server Deploy Wizard'. The dialog is divided into several sections:

- Database:** Contains fields for 'Host' (LOCALHOST\SQLE2017) and 'Database' (DPS). A dropdown menu for 'Microsoft SQL Server' is visible. There is an 'Advanced Settings' button.
- Credentials:** Includes a checkbox for 'Integrated security' (unchecked).
- Management Tools:** Contains fields for 'Username' (VaultOwner) and 'Password' (masked with dots). To the right, there is a section titled 'Using Management Tools Credentials' with buttons for 'Test Server', 'Create Database', 'Test Database', 'Update Database', and 'Email Schema to Support'. A link 'View Database Version' is also present.
- Scheduler Service:** Contains fields for 'Username' (VaultScheduler) and 'Password' (masked with dots). To the right is a button 'Test Scheduler Credentials'.
- Web Application:** Contains fields for 'Username' (VaultRunner) and 'Password' (masked with dots). To the right is a button 'Test Web Application Credentials'.

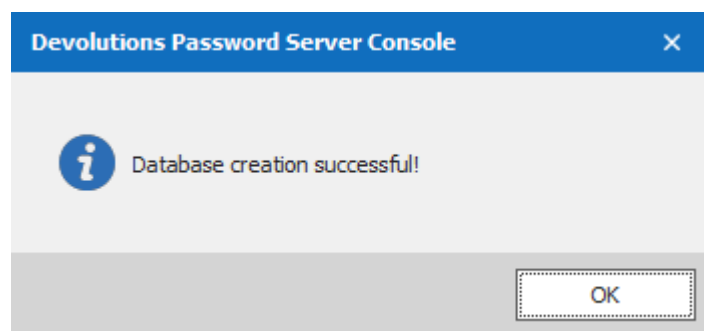
At the bottom right, there are four buttons: 'Previous', 'Next' (highlighted with a dotted border), 'Install', and 'Cancel'.

Database Dialog

7. On the creation of the database, some options can be enabled. For a simple installation, the default selection must be kept. For more information about these options, refer to the [Database](#) topic for further information.

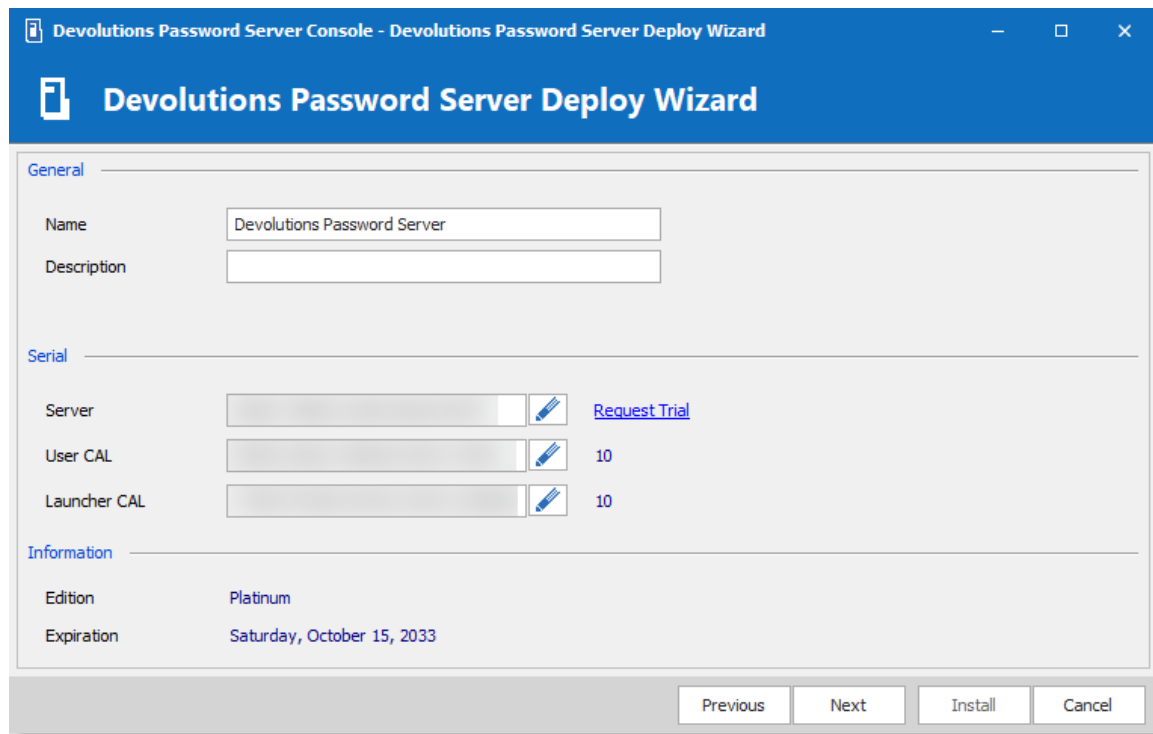


Create daTabase Dialog



Database Creation Successful Dialog

8. Under **General**, enter a custom **Name** and **Description**. Under **Serial**, provide a license serial that has been received by email upon buying the product. If you did not buy any Devolutions Server license yet, you may [Request a 30-days trial](#).



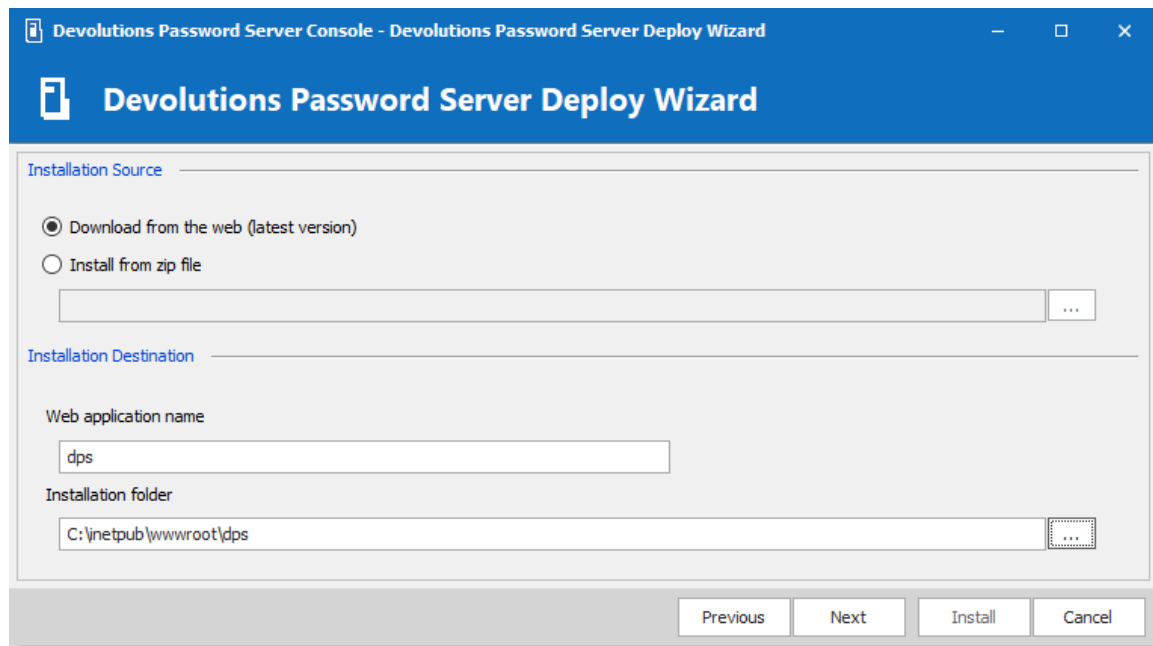
General and Registration Dialog

9. Under **Installation Source**, select to either **download the latest version from the web**, or **install from a local zip file**.

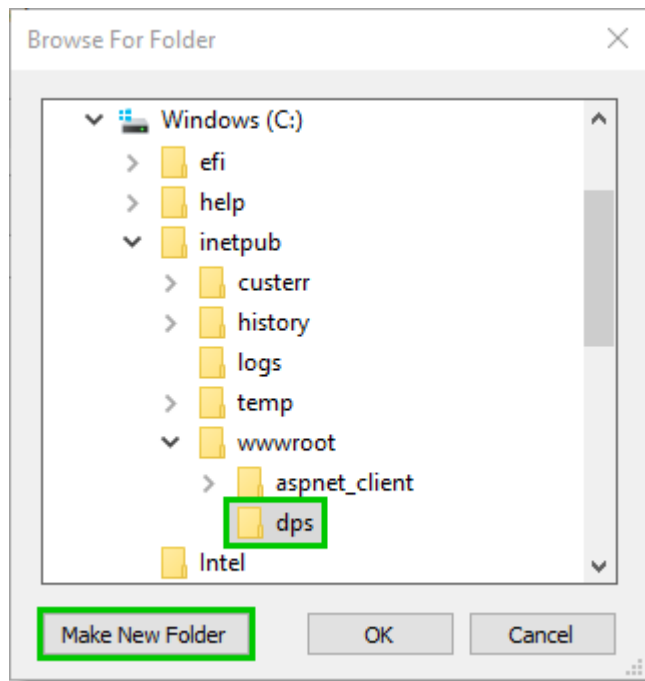
Under **Installation Destination**, select the destination folder, and an IIS virtual directory name. The process to run Web sites has been granted the proper permissions under **c:\inetpub\wwwroot**. We recommend to create a new folder beneath it and create the Devolutions Server instance within this folder.



We do not recommend to set the installation folder to **C:\Program Files** or **C:\Program Files (x86)**. Devolutions Server is a web application and this could result in unwanted behavior and issues because IIS do not have enough permissions to run web applications that are located under those folders.

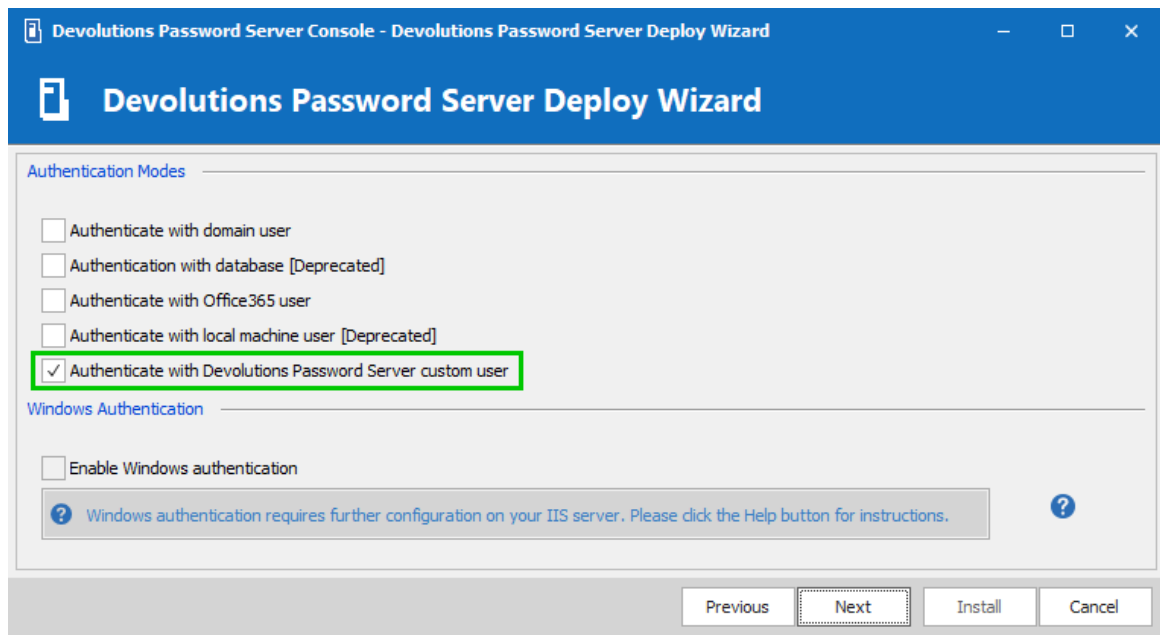


Source and Destination Dialog

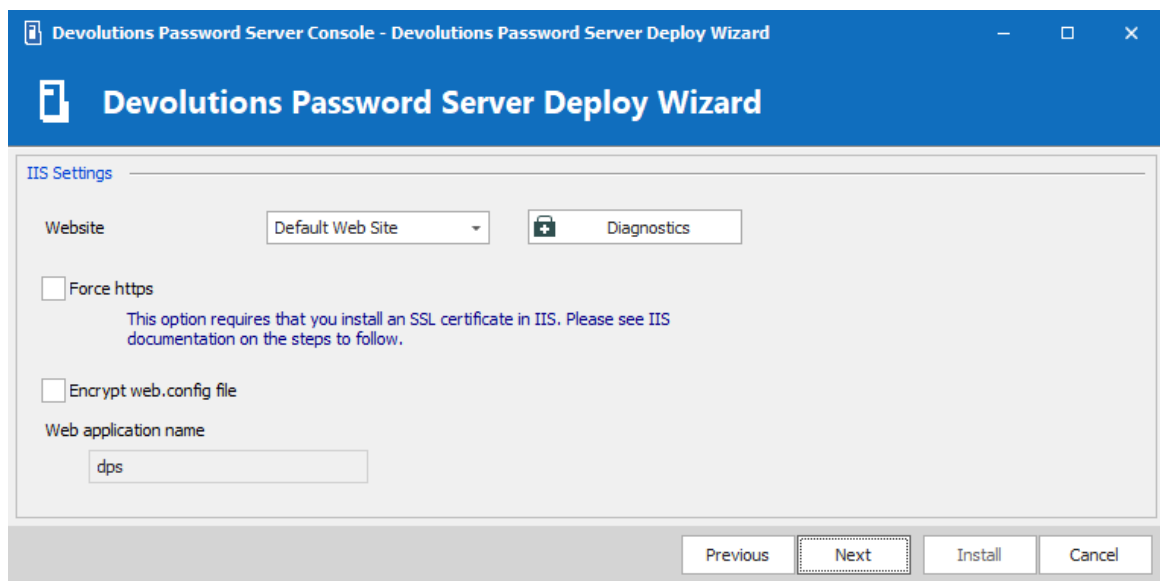


Create and select Folder

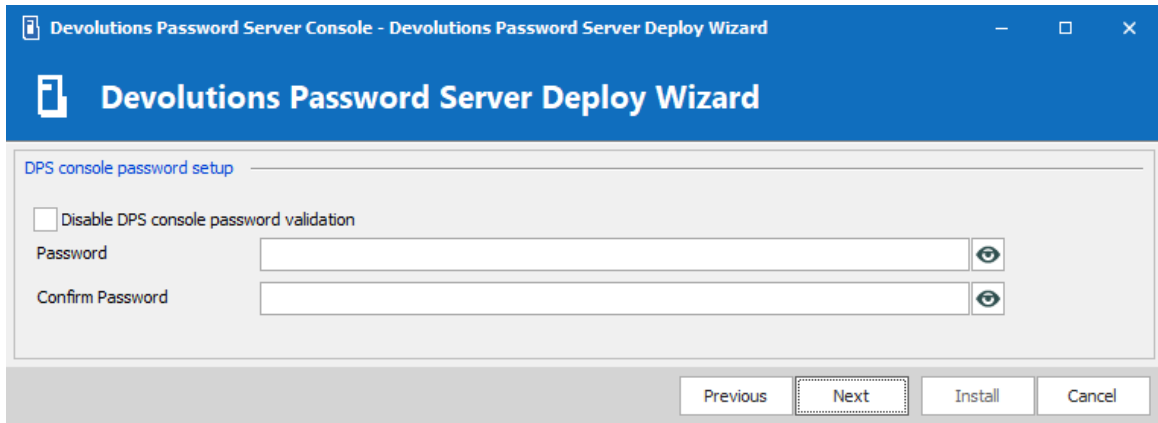
10. Under Authentication Modes, select the modes which users authenticate with. For the initial setup, we recommend enabling **Authenticate with Devolutions Server custom user**. This guarantees connectivity for the first steps and can be disabled later. If you are connected to a domain, please refer to the [Authentication server settings](#) topic for further information.

*Authentication Modes Dialog*

11. Under IIS Settings, select the website used to host the Devolutions Server instance. Make sure the Internet Information Services (IIS) is installed in order to proceed with the installation of Devolutions Server.

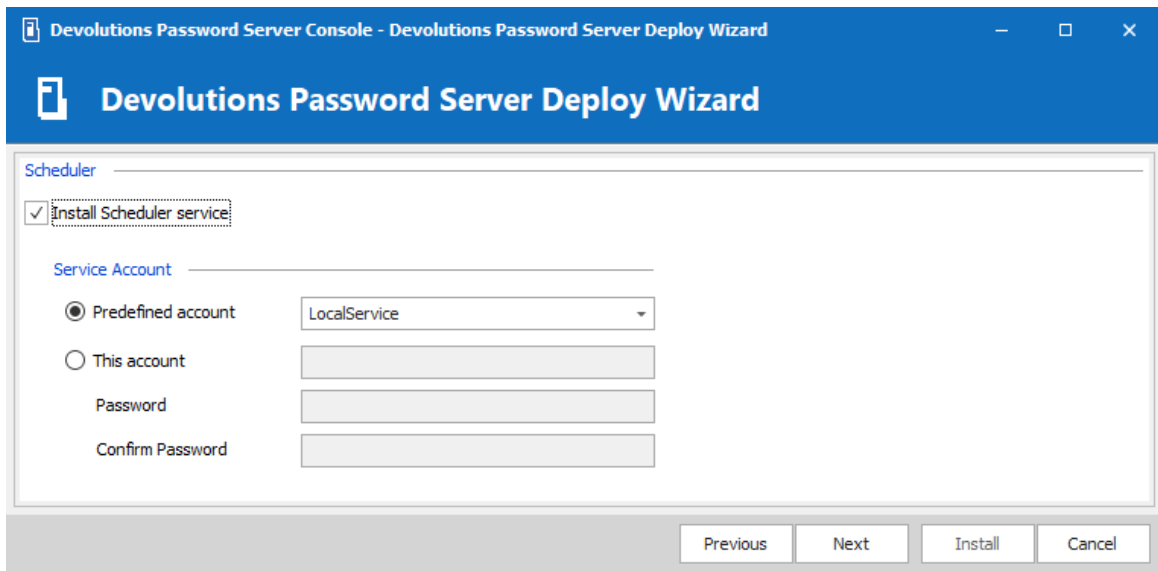
*IIS Settings Dialog*

12. Under DPS console password setup, when configuring a password, the Devolutions Server instance will be protected by a password that will be saved in the database.

The screenshot shows the 'Devolutions Password Server Deploy Wizard' window. The title bar reads 'Devolutions Password Server Console - Devolutions Password Server Deploy Wizard'. The main header is blue with the Devolutions logo and the text 'Devolutions Password Server Deploy Wizard'. Below the header, the section is titled 'DPS console password setup'. It contains a checkbox labeled 'Disable DPS console password validation' which is unchecked. Below this are two text input fields: 'Password' and 'Confirm Password', each with a small eye icon to its right for toggling visibility. At the bottom right, there are four buttons: 'Previous', 'Next' (which is highlighted with a dotted border), 'Install', and 'Cancel'.

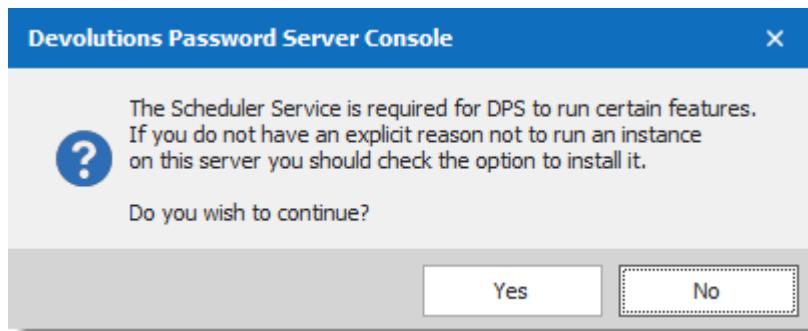
Devolutions Server password protected console

13. Under Scheduler, when enabling the Install Scheduler service option, please set the proper Service Account. The following features depend on the Scheduler : [Backup manager](#), [Domain Users and Roles cache](#), [Office365 Users and Roles cache](#), Email notifications and [Privileged Access Management](#).

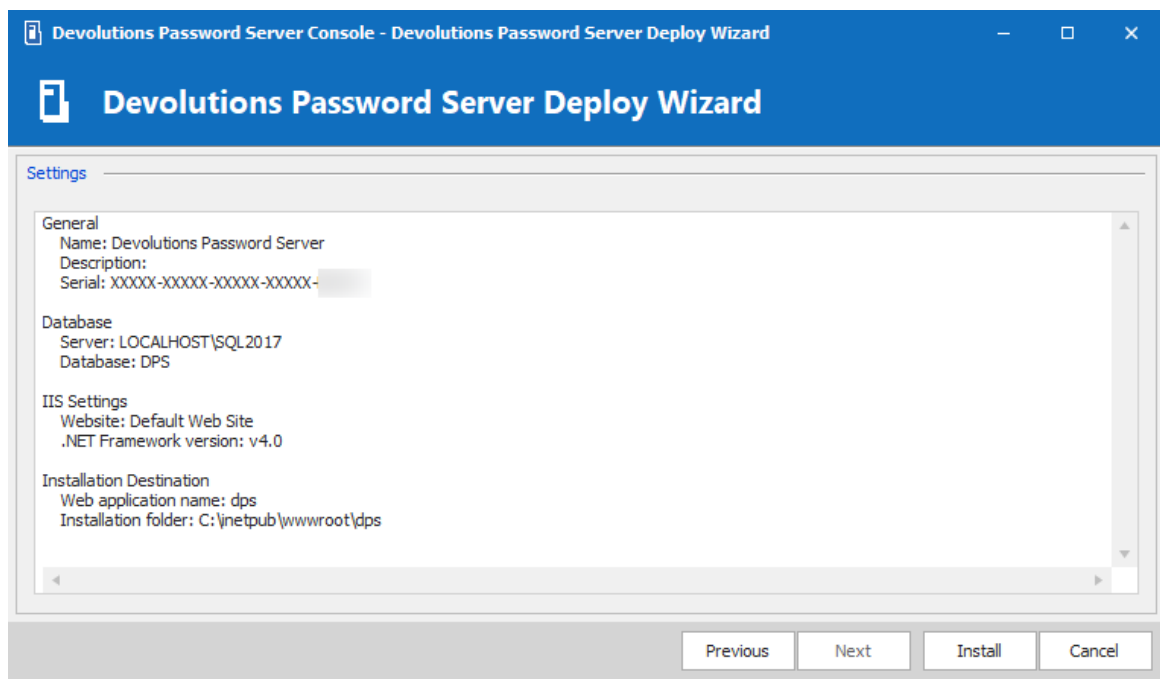
The screenshot shows the 'Devolutions Password Server Deploy Wizard' window at the 'Scheduler' step. The title bar and header are the same as in the previous screenshot. The section is titled 'Scheduler'. It features a checkbox labeled 'Install Scheduler service' which is checked. Below this, under the 'Service Account' section, there are two radio button options. The first is 'Predefined account', which is selected, and it has a dropdown menu showing 'LocalService'. The second is 'This account', which is unselected and has three empty text input fields below it labeled 'Password', 'Confirm Password', and another unlabeled field. At the bottom right, there are four buttons: 'Previous', 'Next' (highlighted with a dotted border), 'Install', and 'Cancel'.

Scheduler Dialog

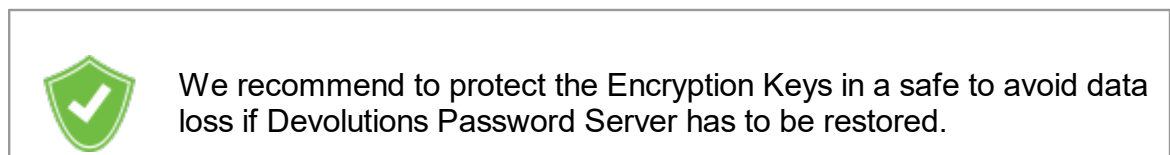
14. Choosing to not install the Scheduler, you will get the following warning message.

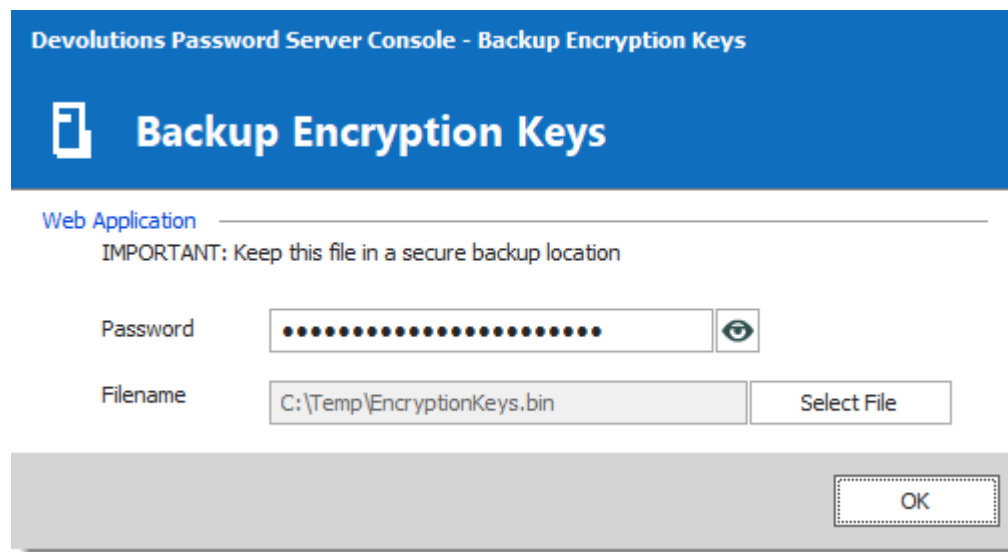
*Scheduler Warning*

15. Under **Settings**, validate the configuration and click **Install**.

*Settings Dialog*

16. The last step is to save the Encryption Keys file in a folder.

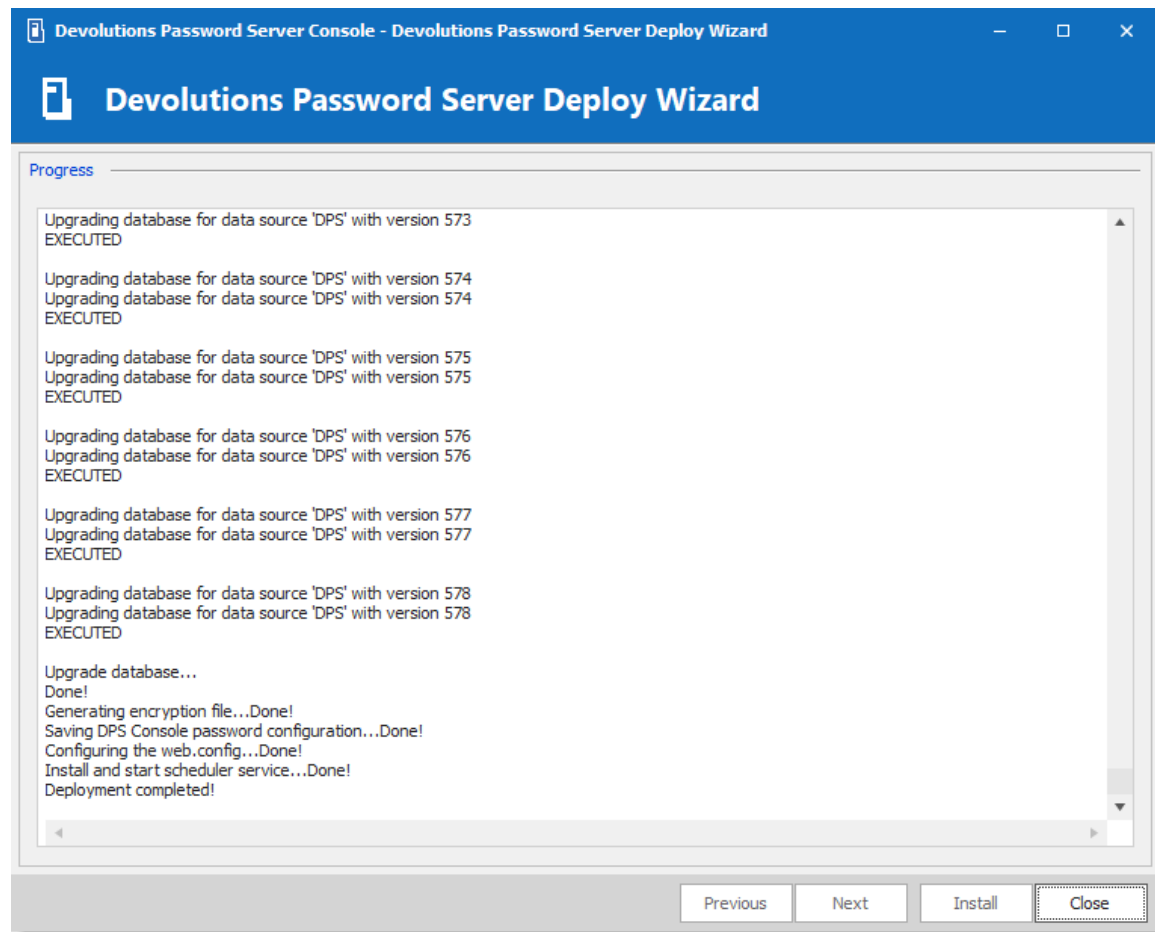




The screenshot shows a Windows-style dialog box titled "Devolutions Password Server Console - Backup Encryption Keys". The title bar is blue with a white icon of a document with a key. Below the title bar, the text "Web Application" is followed by a horizontal line. Below this line, the text "IMPORTANT: Keep this file in a secure backup location" is displayed. There are two input fields: "Password" and "Filename". The "Password" field contains a series of black dots and has a small eye icon to its right. The "Filename" field contains the text "C:\Temp\EncryptionKeys.bin" and has a "Select File" button to its right. At the bottom right of the dialog box is an "OK" button.

Backup Encryption Keys Dialog

Once the installation is complete, a summary indicates if the Devolutions Server has been deployed correctly.



Progress Installation Dialog

CREATE THE INITIAL ADMINISTRATOR


Create at least one administrator user account.

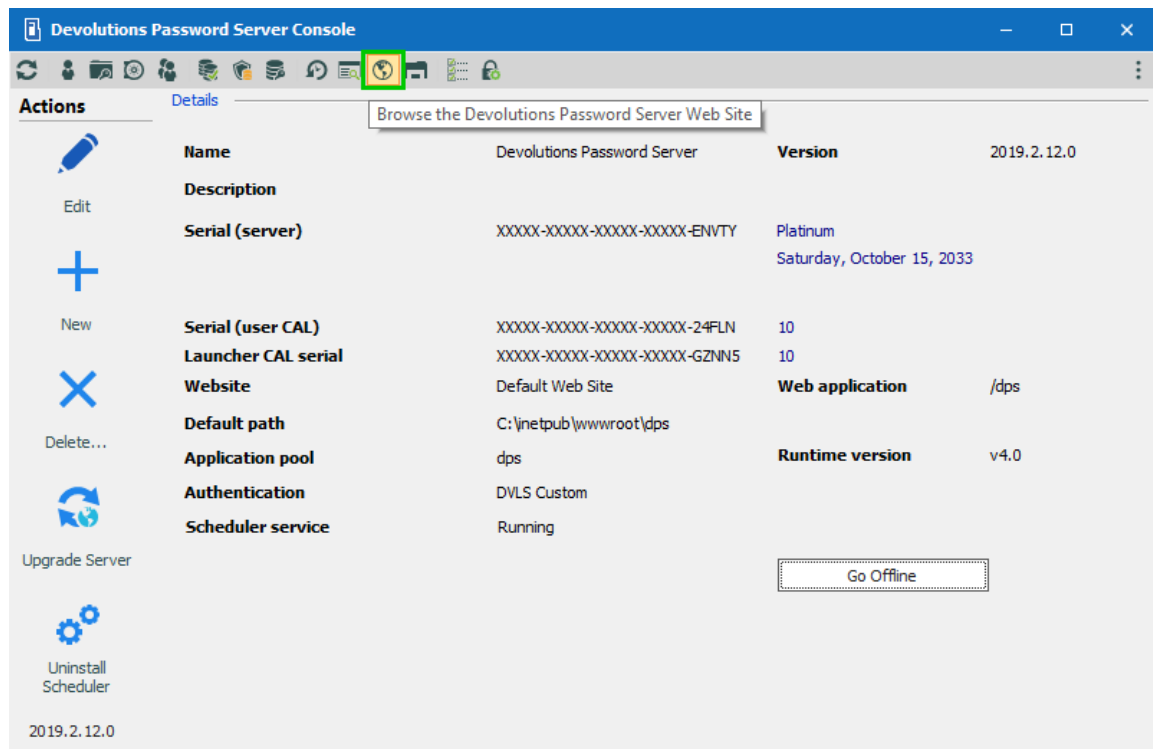


You must create an administrator account if you've enabled the Devolutions Server Authentication mode. In other cases, the account name must match with the chosen authentication mode. If you are unsure of the result, also enable Devolutions Server authentication, create an administrator account and grant the Administration privilege to the account. Please refer to [User Management](#) for further information about creating user accounts.

After the successful authentication with the other model, the Devolutions Server user account will have been created and you will be able to see how to format your account names. You can then disable the Devolutions Server authentication model. Please see Automatic User Account Creation section in the topic [Authentication](#).

TEST THE INSTALLATION

To test the server installation, navigate to the instance URL (e.g.: http://<Machine_Name>/<InstanceName>) with any web browser or click on the **Open in web browser**  button in the Devolutions Password Server Console.



Devolutions Password Server Console

To test the connection from a client by creating a data source in Remote Desktop Manager.

3.4 Upgrading Devolutions Server

UPGRADE



Install the proper version of Devolutions Password Server Console before upgrading the Devolutions Server web application. It is available on the [Download page](#).



Since Devolutions Server 2019.x, many features can only be managed from the web interface. Please see [Administration - Password Server Settings](#).

It is highly recommended as a best practice to first deploy the new version of Devolutions Server to a staging instance and verify its stability before deploying it to your whole organization. If you do not have a staging instance we then recommend a limited roll-out to ensure the work flow is supported to your satisfaction prior to impacting your whole team.



These steps are intended to be achieved on a single server or a basic [topology](#). If your environment differs from these topologies, please contact us and we will guide you on how to upgrade Devolutions Server.

WORKFLOW



We highly recommend to test the upgrade process in a staging/test environment before upgrading your production instance.



The upgrade steps will be performed with Devolutions Password Server Console. You will need to upgrade your copy to the latest version that is matched with the target version of Devolutions Server that you are preparing to install. Please follow the steps carefully.



If you have elected to use **Integrated Security** for connecting to the database, you must perform the upgrade using a Windows user account that has full rights on the database.



If you have set the [Security Provider](#) Passphrase v1 on your current Devolutions Server, specific operations will need to be done before the upgrade. Please contact us for further details.



We recommend doing a backup of the [Encryption Keys](#) before any operation that could modify the information of the database or before the upgrade of Devolutions Password Server. Protect the Encryption Key in a safe to avoid data loss if Devolutions Password Server has to be restored.

PREPARATION PHASE

- Ensure that the instance users have the offline mode enabled and that they all perform a full refresh of the cache (CTRL+F5).
- Have your team switch to the offline mode, allowing them to work while the system is down.
- Update the Maximal version of Remote Desktop Manager in **Administration - System Settings - Version Management - Maximal version**, if this option was set before the upgrade.

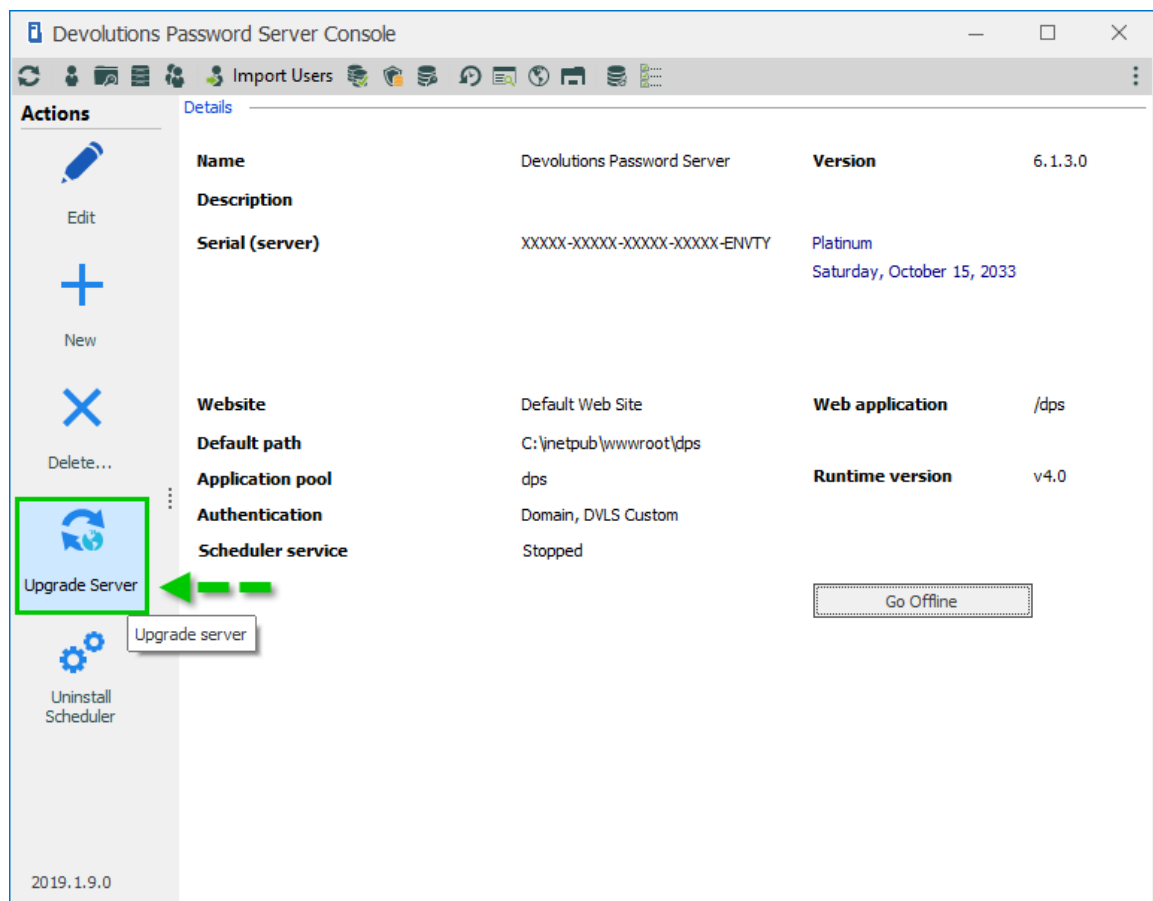
PHASE 1

- Perform a full backup of the database, take precautions against that backup file being deleted by a maintenance plan.

- Archive the content of the folder containing the Devolutions Server instance, move to a safe place.
- Install the proper version of Devolutions Password Server Console. In each of the sub-topics related to a specific version of Devolutions Server you will find the version of the client that you need.
- Devolutions Password Server Console must be run with elevated privileges.

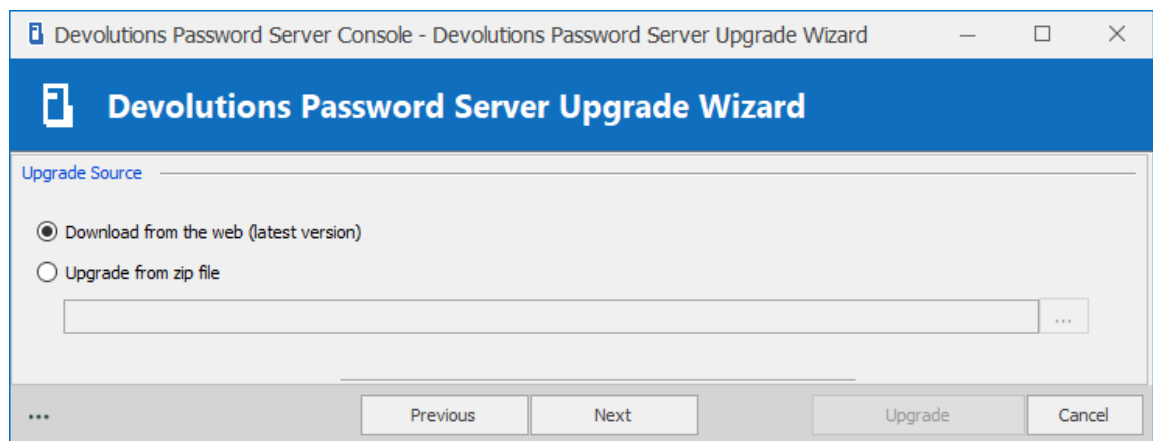
PHASE 2

1. Open the [Devolutions Server Console](#).
2. Select the instance that you wish to upgrade.
3. Set the instance in **Offline Mode** with the **Go Offline** button. On a High Availability/Load Balancing topology, all instances must be set to Offline mode before
4. Click the **Upgrade Server** button.



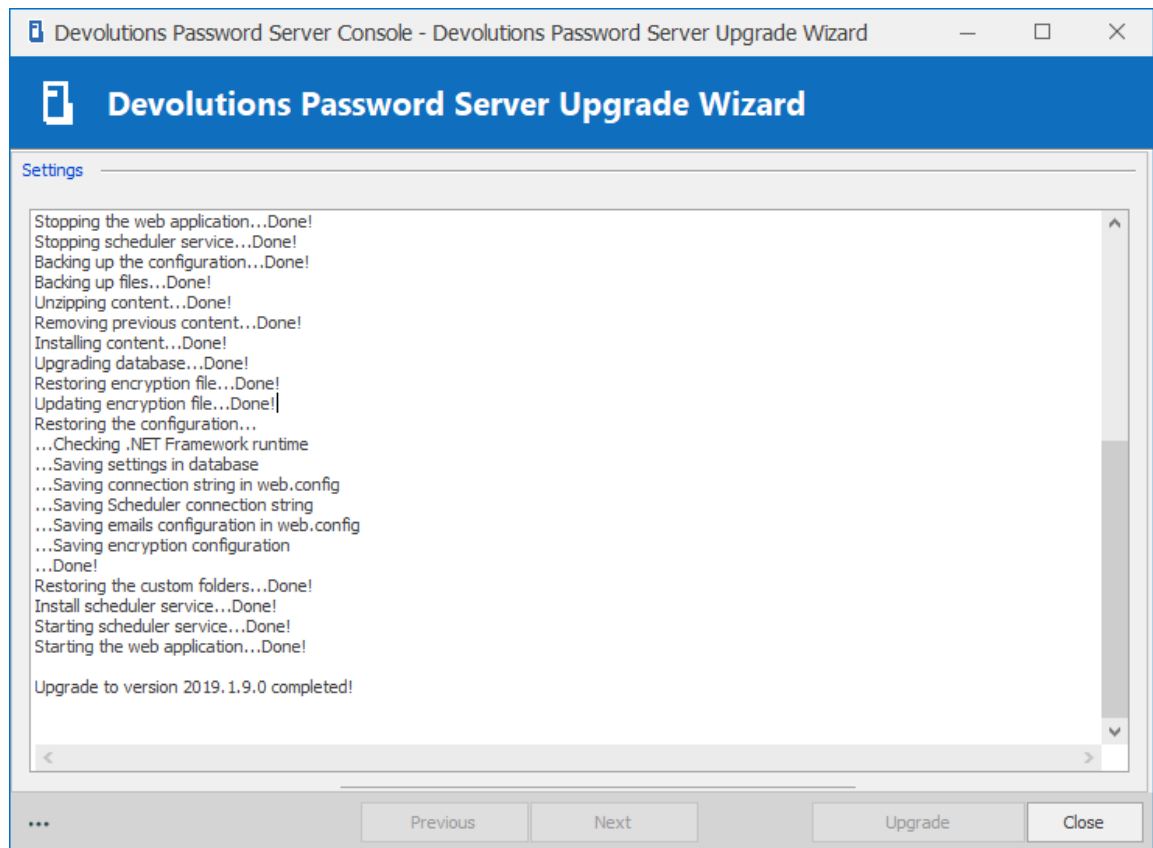
Devolutions Password Server Console

5. Select the **Upgrade Source**. You can either use the latest General Availability release that is available online automatically or specify the path to a zip file that you have downloaded yourself. Use this for beta releases or for earlier versions.



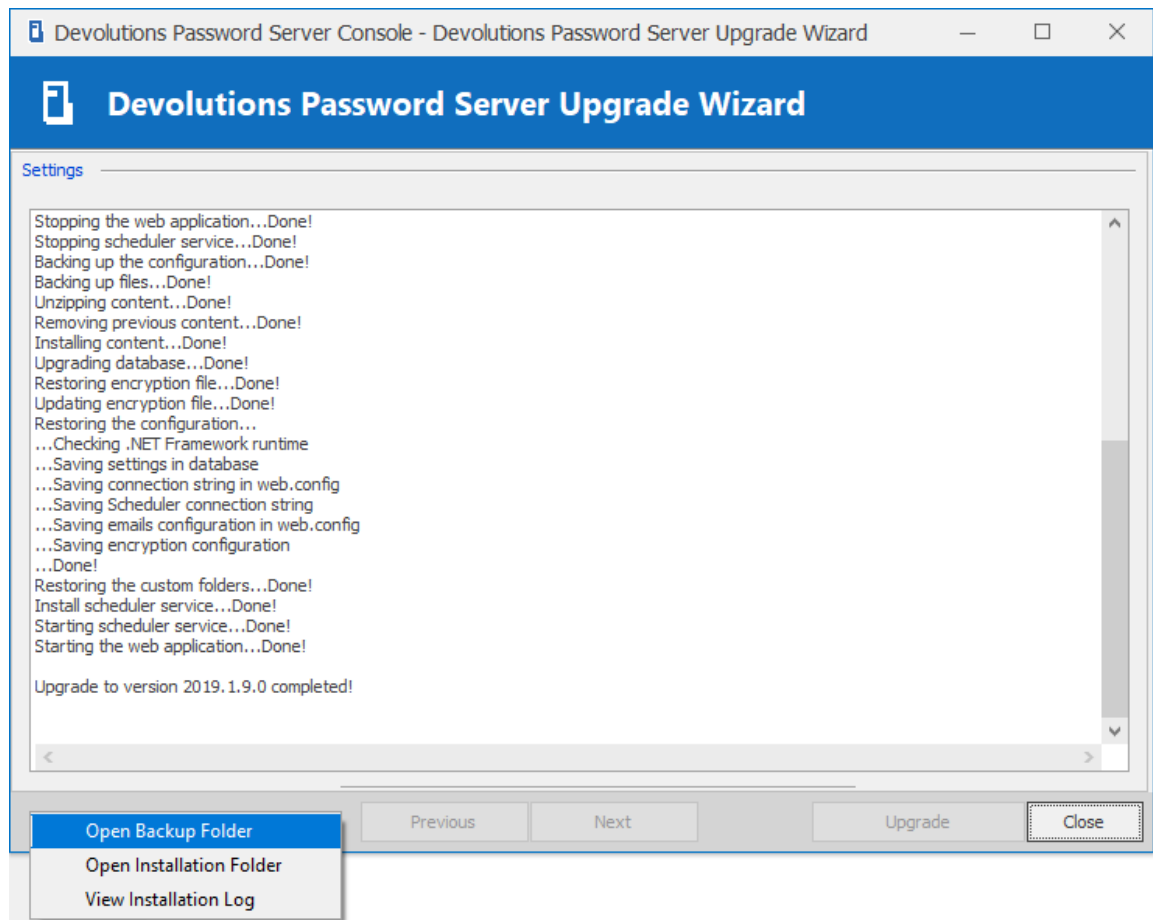
Devolutions Server Upgrade Wizard

6. Press **Next**.
7. Review the summary and press **Upgrade** if you are satisfied.



Upgrade completed

8. Since Devolutions Server version 4.6.0.0, it is possible to access the **Backup Folder**, the **Installation Folder** or **View Installation Log** from the **More Options** button in the lower left corner of the Devolutions Server **Upgrade Wizard** dialog.



FINAL PHASE



The **Backup Folder** contains information about the configuration of the Devolutions Server instance prior to the upgrade. After a successful upgrade, you must ensure the content is either moved to a safe place, or deleted.



Our support department gets more and more urgent requests for assistance because of a rogue admin upgrading his own copy of Remote Desktop Manager and introducing a schema update for some new feature. This may prevent other users from using the system. We strongly recommend setting both the Maximal and Minimal versions allowed to connect to your instance.

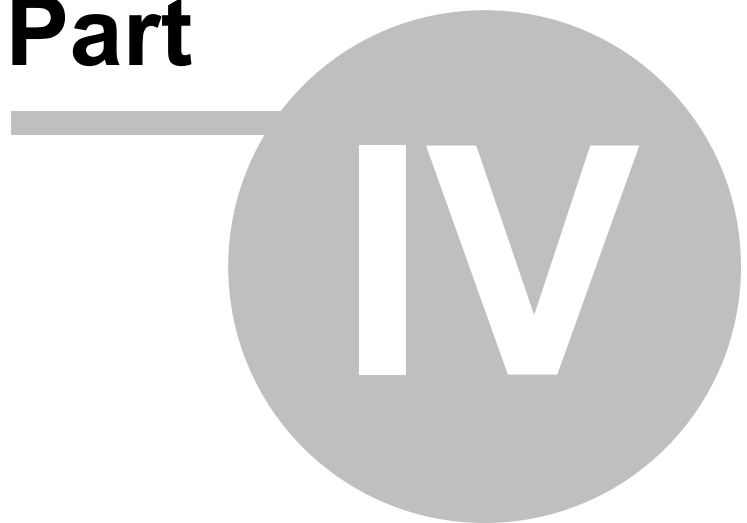


If you have elected to use the Integrated Security for connecting to the database in the [Database](#) tab, ensure that the IIS Application Pool Identity and Scheduler accounts have enough privileges on the database. After an upgrading to a new version, new permissions are possibly required. Please contact us about the new permissions list.

- Have a user upgrade his workstation with the version of Remote Desktop Manager supported by the Devolutions Server version and test connectivity with the server instance.
- When you are satisfied with your tests, have the rest of the staff upgrade to the same version of Remote Desktop Manager.
- Update the Maximal/Minimal version of Remote Desktop Manager in ***Administration - System Settings - Version Management***
- Move or delete the **Backup Folder**, it is located in the **%TMP%\DVLS** folder of the current user profile. Newer versions of Remote Desktop Manager add a suffix to indicate a sequence.

Management

Part



4 Management

4.1 Devolutions Password Server Console

DESCRIPTION

Because Devolutions Server is in fact a web application, the management interface is provided by the Devolutions Password Server Console.

USAGE



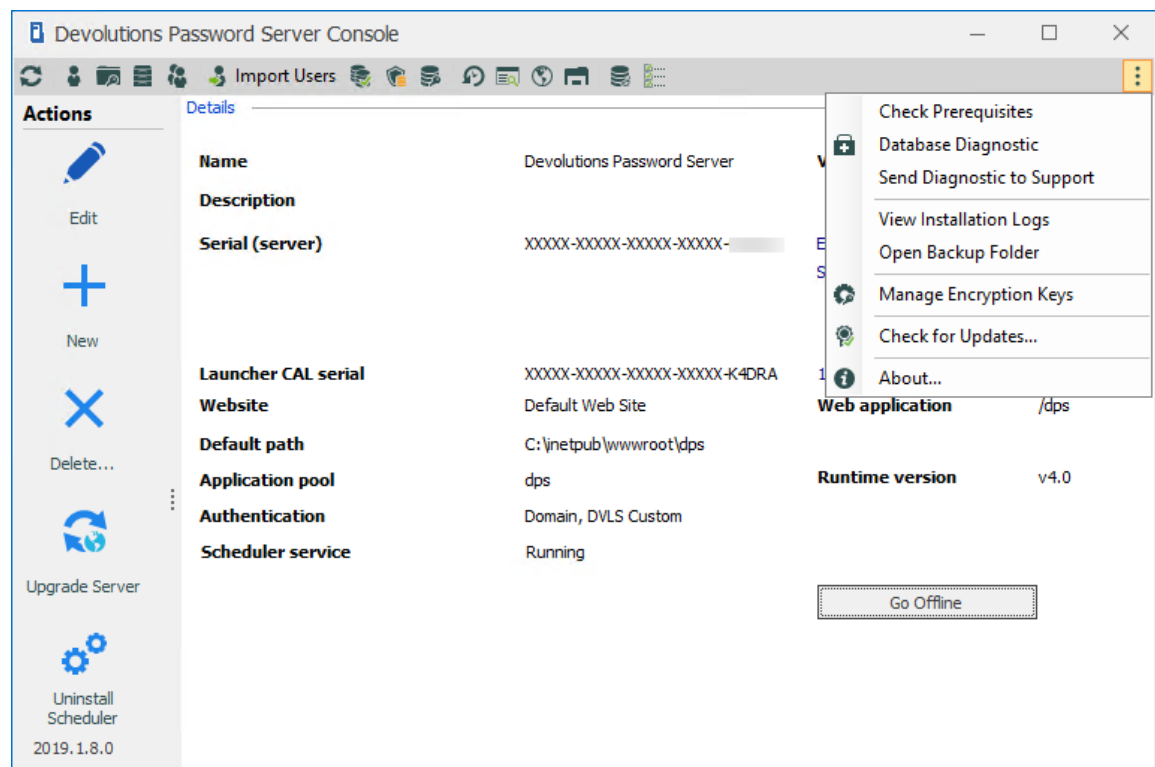
The Devolutions Password Server Console is now offered as a stand alone application. It is now available on the [Download page](#).



Since Devolutions Server 2019.x, many features can only be managed from the web interface. Please see [Administration - Password Server Settings](#).

The Devolutions Password Server Console manages the IIS metabase, it must be started with elevated privileges when the console needs to be used. Elevated privileges are granted when you use "**Run as administrator**" to launch the application. You can modify the shortcut to always start it in this manner.

CONSOLE



Devolutions Password Server Console

SETTINGS

SECTION	DESCRIPTION
Actions pane	Contains the buttons for the main controls. Edit , New , Delete, Upgrade Server and Uninstall Scheduler.
Commands	The menu at the top contains the Commands accessible.
Advanced menu	The menu at the top right contains the Advanced features.

4.1.1 Devolutions Server Settings

4.1.1.1 General

DESCRIPTION

The General tab contains the basics information of the Devolutions Server instance such as the Name, Description, Serial Keys, etc.

The screenshot shows the 'Devolutions Password Server Console - Password Server Settings' window. The 'General' tab is selected in the left sidebar. The main area is divided into sections: 'General' with fields for 'Name' (filled with 'Devolutions Password Server') and 'Description' (empty), and a checkbox for 'Enable new version mode'. The 'Serial' section contains three rows: 'Server' with a masked serial key and a 'Request Trial' link, 'User CAL' with a masked key and the value '10', and 'Launcher CAL' with a masked key and the value '10'. The 'Information' section shows 'Edition' as 'Platinum' and 'Expiration' as 'Saturday, October 15, 2033'. At the bottom, there is a 'Search property' field, a magnifying glass icon, and 'Save' and 'Cancel' buttons.

General Tab

SETTINGS

GENERAL

OPTION	DESCRIPTION
Name	Enter the name for your server, it will be displayed in the Content area.
Description	Enter a short description or additional information.

SERIAL

OPTION	DESCRIPTION
Server	Insert your serial registration number.
Request trial	This will redirect you to our Devolutions Server page to request a free 30 days trial.
User CAL	Insert your Client Access License key.
Launcher CAL	Insert your Launcher key.

INFORMATION

OPTION	DESCRIPTION
Edition	Display the Devolutions Server Edition according to your Server license key.
Expiration	Expiration date of the product.

4.1.1.2 Database

DESCRIPTION

The Database tab contains the information of the SQL Server, the SQL credentials information and the database name used by Devolutions Server.

The screenshot shows the 'Password Server Settings' window with the 'Database' tab selected. The left sidebar contains a tree view with 'General', 'Database', 'Authentication', 'Domain', 'Office365', 'IIS', and 'Advanced'. The main area is divided into sections: 'Database' (Host: 'VWINDSRV-SQL\SQL2016', Database: 'DPS', and a dropdown menu showing 'SQL Server', 'SQL Server', and 'SQL Azure'), 'Credentials' (with an 'Integrated security' checkbox), 'Management Tools' (Username: 'VaultOwner', Password: masked), 'Scheduler Service' (Username: 'VaultScheduler', Password: masked), and 'Web Application' (Username: 'VaultRunner', Password: masked). On the right, there are buttons for 'Test Server', 'Create Database', 'Test Database', 'Update Database', 'Email Schema to Support', and 'View Database Version'. At the bottom, there is a 'Search property' field and 'Save' and 'Cancel' buttons.

Database Tab

SETTINGS

DATABASE

OPTION	DESCRIPTION
Host	Name of the host where the database will be stored.
SQL Server / SQL Azure	Choose the database host type.
Database	Name of the database on the server.

OPTION	DESCRIPTION
Advanced Settings	Access the Advanced Settings .
Test Server	Test the connection with the server to validate if the proper information has been provided.
Create Database	If the database doesn't already exist you can create one directly from here. In order to use integrated security correctly, the database must be created with at least db_owner rights.
Test Database	Test the connection with the database to validate if the proper information has been provided.
Update Database	Update the database on the server.
Email Schema to Support	Directly sends your schema to the Devolutions Support team.
View database version	View what is your current database version.

CREDENTIALS

Note that the Integrated Security or Credentials settings affect how the Devolutions Server communicates with the SQL database. These options do not have any impact on how users will authenticate on the Devolutions Server instance.

OPTION	DESCRIPTION
Integrated security	Specify to use Windows Integrated Authentication for authenticating to the database. In order for integrated security to be used to connect to the database, you must set a domain account as the Application Pool identity in the IIS Manager.

OPTION	DESCRIPTION
Management Tools	Credentials that allows the Devolutions Password Server Console to communicate with the SQL database. Must be a SQL account.
Scheduler Service	Credentials used for the Scheduler features (Backup manager, Email Notifications, Secure Messaging, Domain Users and Roles cache, Azure AD cache). Must be a SQL account.
Test Scheduler Credentials	Test against the SQL server the credentials set in Scheduler Service.
Web Application	Credentials used for the Web Application to communicate with the SQL database. Must be a SQL account.
Test Web Application Credentials	Test against the SQL server the credentials set in Web Application.

4.1.1.2.1 Advanced Settings

DESCRIPTION

The Advanced Settings contains advanced parameters that are used for the SQL database connection string.

Devolutions Password Server Console - SQL Server

SQL Server

☐ Use SQL Server encrypted connection

☐ Trust server certificate

Failover partner

Connection minimum pool size

Connection maximum pool size

Connection retry count

Connection retry interval

Connection timeout

OK Cancel

Advanced Settings Dialog

SETTINGS

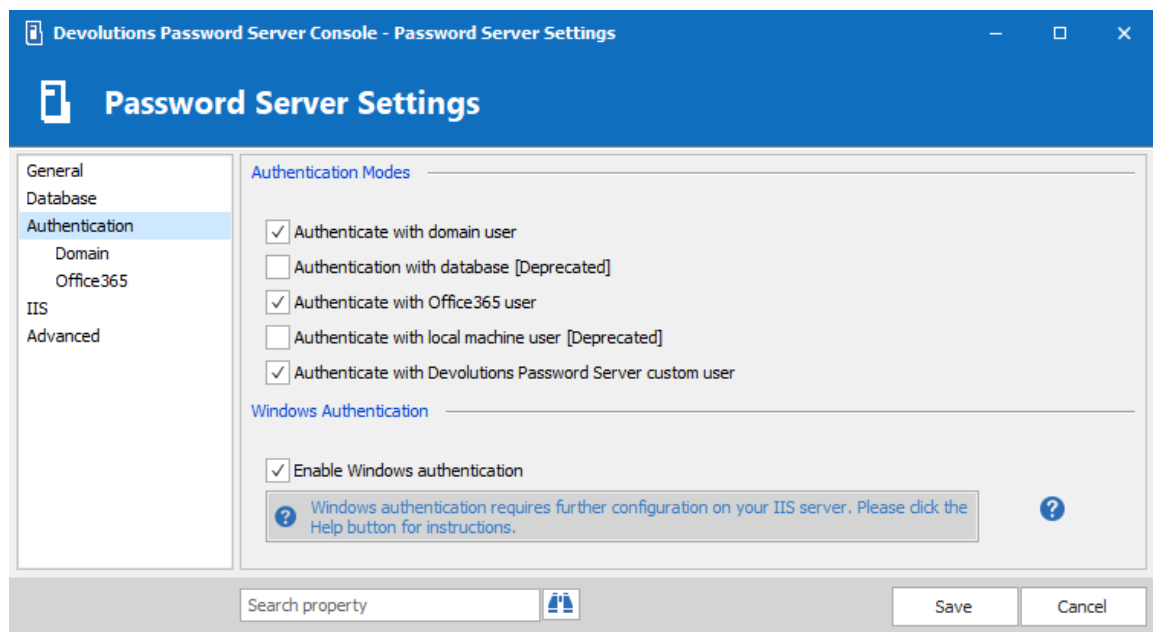
OPTION	DESCRIPTION
Use SQL Server encrypted connection	Use SSL to encrypt communication with the database.
Trust server certificate	Always trust the server certificate.
Failover partner	The name of the failover partner server if database mirroring is configured. This is used only for the initial connection as the principal server will return a name which will replace the configured value when different.
Connection minimum pool size	The minimum number of connections that are allowed in the pool.

OPTION	DESCRIPTION
Connection Maximum pool size	The maximum number of connections that are allowed in the pool.
Connection retry count	Controls the number of reconnection attempts after the client identifies an idle connection failure. Valid values are 0 to 255. The default is 1. 0 means do not attempt to reconnect .
Connection retry interval	Specifies the time between each connection retry attempt (ConnectRetryCount). Valid values are 1 to 60 seconds (default=10), applied after the first reconnection attempt. When a broken connection is detected, the client immediately attempts to reconnect; this is the first reconnection attempt and only occurs if ConnectRetryCount is greater than 0. If the first reconnection attempt fails and ConnectRetryCount is greater than 1, the client waits ConnectRetryInterval to try the second and subsequent reconnection attempts.
Connection timeout	The length of time (in seconds) to wait for a connection to the server before terminating the attempt and generating an error.

4.1.1.3 Authentication

DESCRIPTION

Select the type of authentication method used by your users to connect to the Devolutions Server. As best practice we would strongly recommend the use of Domain Authentication method as it can be integrated with Active Directory Group and makes it easier to manage.

*Authentication Tab*

SETTINGS

AUTHENTICATION MODES

OPTION	DESCRIPTION
Authenticate with domain user	The domain is used to authenticate the user.
Authenticate with database user	The database is used to authenticate the user. This authentication method is now identified as deprecated.
Authenticate with Office365 user	AzureAD is used to authenticate the user.
Authenticate with local machine user	The application allows a local user to be authenticated on the server. This authentication method is now identified as deprecated.

OPTION	DESCRIPTION
Authenticate with Devolutions Server custom user	The Devolutions Server is used to authenticate the user. You must create the initial user through the console.

WINDOWS AUTHENTICATION

OPTION	DESCRIPTION
Enable Windows Authentication	The application will use the current Windows authenticated user to authenticate to the Devolutions Server instance.

4.1.1.3.1 Domain

DESCRIPTION

The domain is used to authenticate the user. This is the most secure, flexible and easiest to manage. No need to sync users between the domain and Devolutions Server. On first use of the Devolutions Server data source, the user will be created and be given access rights according to their role in the organization as defined on the domain. You simply need to grant appropriate permissions to your roles in Devolutions Server. Upon authentication we will validate the AD groups to which the user belongs and for any that have a corresponding role we will grant the permissions to the user.

The screenshot shows the 'Password Server Settings' window with the 'Domain' tab selected in the left sidebar. The main panel is divided into several sections:

- Domain Authentication:** Includes a 'Domain' text field with 'windjammer.loc', an 'Administration credentials' text field with 'david@windjammer.loc' and a clear button, and an unchecked checkbox for 'Allow logins using email address'.
- LDAPS:** Includes a checked checkbox for 'Enable LDAPS', a 'Port' section with 'Default' selected (radio button) and a 'Custom' option with a value of '0' in a spinner box.
- Automatic User Creation:** Includes a checked checkbox for 'Auto create domain users in database', a checked checkbox for 'Create read-only user', a 'Default Vault' dropdown menu set to 'Default', and an 'Only from this AD group' text field with 'RDM Users' and a clear button. Below this is a 'Username Format' section with 'UPN' selected (radio button) and 'Netbios' and 'Username' as other options.
- Multi Domain:** Includes a checked checkbox for 'Multi domain' and a 'Trusted domains' text field with 'nino.windjammer.loc' and a clear button.
- Domain Users And Roles Cache:** Includes a checked checkbox for 'Enable domain cache feature' and an 'Update users and groups data every:' section with a spinner box set to '0' for 'Hours' and a spinner box set to '30' for 'minutes'.

At the bottom, there is a 'Search property' text field, a 'Save' button, and a 'Cancel' button.

Domain Tab

SETTINGS

DOMAIN AUTHENTICATION

OPTION	DESCRIPTION
Domain	Specify the remote computer domain name.

OPTION	DESCRIPTION
Administration credentials	Add the credentials of a domain or service account to access the Active Directory forest and obtain user account information through LDAP queries. This is needed when the server hosting the instance is not located on the domain. This account needs to be a member of the Account Operators AD group in order to have enough permissions to retrieve user account information and group memberships.
Allow logins using email address	Allow users to use their email address to connect to the Devolutions Server instance. The email address field must be filled in the User Management.

LDAPS

OPTION	DESCRIPTION
Enable LDAPS	Enable the LDAP over SSL communication.
Default	LDAPS default communication port.
Custom	Set a specific port value.

AUTOMATIC USER CREATION

OPTION	DESCRIPTION
Auto create domain users in database	Automatically create the domain user account in the the database on the first login attempt.
Create read-only user	When this option is enabled, the user account will be created as a Read only user type account.

OPTION	DESCRIPTION
Default Vault	Will give access to that Vault to the user.
Only from this AD group	Will create automatically the user only if he is a member of this AD group.
Username Format	<p>Select the username format that will be created in the database.</p> <ul style="list-style-type: none">• UPN : The user will be created using the UPN format ex: bill@windjammer.loc.• NetBios : The user will be created using the NetBios format ex: WINDJAMMER\bill.• Username : The user will be created using the SAM account name.

MULTI DOMAIN



The Multi Domain feature requires the Devolutions Server Platinum Edition license. Currently, it is only working with trusted domains that belong to the same AD Forest.

OPTION	DESCRIPTION
Multi domain	Enable the Multi domain feature.
Trusted domains	Add your trusted domains.

DOMAIN USERS AND ROLES CACHE

OPTION	DESCRIPTION
Enable domain cache feature	Activate the domain cache feature.
Update users and groups data every:	Set the hours and minutes period that the Domain Users and Roles Cache will be refreshed. When enable, the default value is set to 30 minutes.

4.1.1.3.2 Office365

DESCRIPTION



Microsoft Azure Active Directory subscription is required to configure Office365 authentication in Devolutions Server. You need to create three new app registrations in Microsoft Azure Active Directory before completing the authentication settings. For more information about the app registrations, see [Azure portal configuration guide for Office 365 authentication](#).

HOW TO CONFIGURE OFFICE 365 AUTHENTICATION

Overview about Office365 configuration: see [knowledge base article](#) for more information

The Office365 tab allows Devolutions Server to authenticate users using Office365 authentication. All fields are mandatory.

The screenshot shows the 'Password Server Settings' window with the 'Office365' tab selected in the left sidebar. The main content area is titled 'Office365 Parameters' and contains several sections:

- Tenant ID:** A text field containing '4a'.
- Native application (RDM):**
 - Client ID:** A text field containing 'a2'.
 - Resource ID:** A text field containing '00'.
 - Redirect URI:** A text field containing 'http://'.
- Web application:**
 - Client ID:** A text field containing 'd9'.
- Users and Roles Cache:**
 - Client ID:** A text field containing '35'.
 - Redirect URI:** A text field containing 'http://'.
 - Secret key:** A text field containing a series of dots.
- Automatic User Creation:**
 - ☒ Auto create Office365 users
 - ☐ Create read-only user
 - Default Vault:** A dropdown menu set to 'Default'.
- Office365 Users And Roles Cache:**
 - Update users and groups data every:** A section with two spinners: '0' Hours and '30' minutes.
 - Test Connection:** A button.

At the bottom of the window, there is a 'Search property' text box, a 'Save' button, and a 'Cancel' button.

Office365 Tab

SETTINGS

OFFICE365 PARAMETERS

OPTION	DESCRIPTION
TenantID	The TenantID is the Directory ID of the Azure Active Directory.

Native application (RDM)	DESCRIPTION
ClientID	Application ID of the Azure AD application.
Resource ID	resourceAppid from the Manifest of the Azure AD application.
Redirect URI	Redirect URI from the Azure AD application.

Web application	DESCRIPTION
ClientID	Application ID from the web app section of the Azure AD application.

Users and Roles Cache	DESCRIPTION
Client ID	Application ID of the Azure AD application.
Redirect URI	Redirect URI from the Azure AD application.
Secret key	Key from the Password generated in Settings - Keys of the Azure AD application.

AUTOMATIC USER CREATION

OPTION	DESCRIPTION
Auto create Office365 users	Automatically create the Office365 user account in the database on the first login attempt.

OPTION	DESCRIPTION
Create read-only user	Set the user account as a read-only account.
Default Vault	Will give access to that Vault to the user.

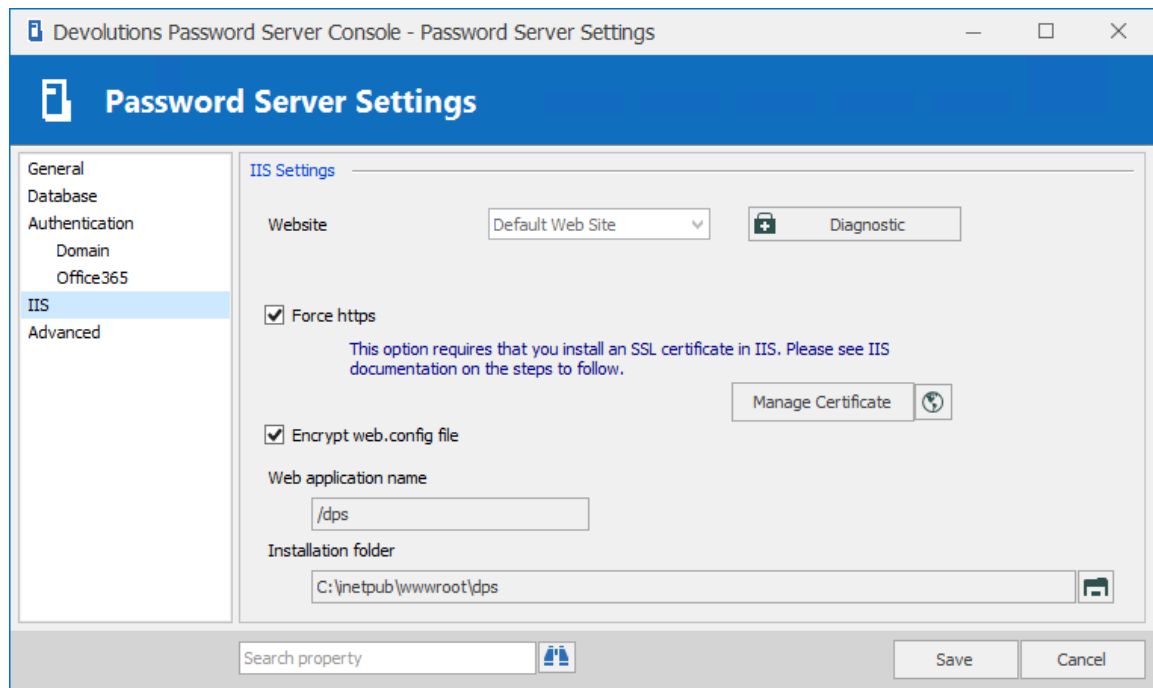
OFFICE365 USERS AND ROLES CACHE

OPTION	DESCRIPTION
Update users and groups data every:	Set the hours and minutes period that the Office365 Users and Roles Cache will be refreshed. Default value is set to 30 minutes.

4.1.1.4 IIS

DESCRIPTION

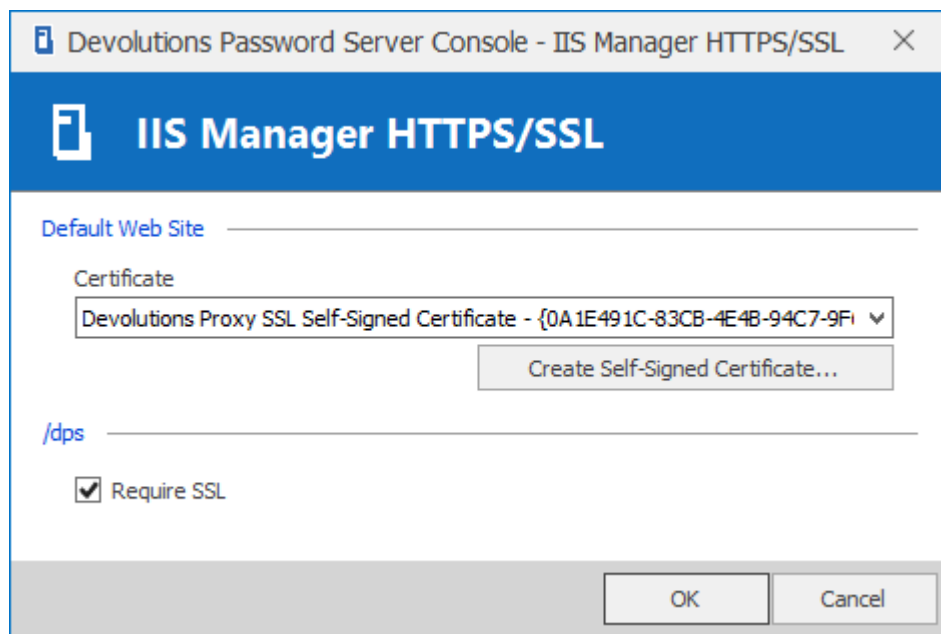
The IIS settings are part of your prerequisite at the installation level. Most of what is found in this tab is automatically filled in by the information given while setting up your Devolutions Server, the IIS Settings tab is used more as an informative source rather than configuration.

*IIS Tab*

SETTINGS

OPTION	DESCRIPTION
Force https	Force the use of the https instead of the http.
Encrypt web.config file	Activate this option if you wish to add an extra layer of security to your configuration by encrypting your file.

MANAGE CERTIFICATE

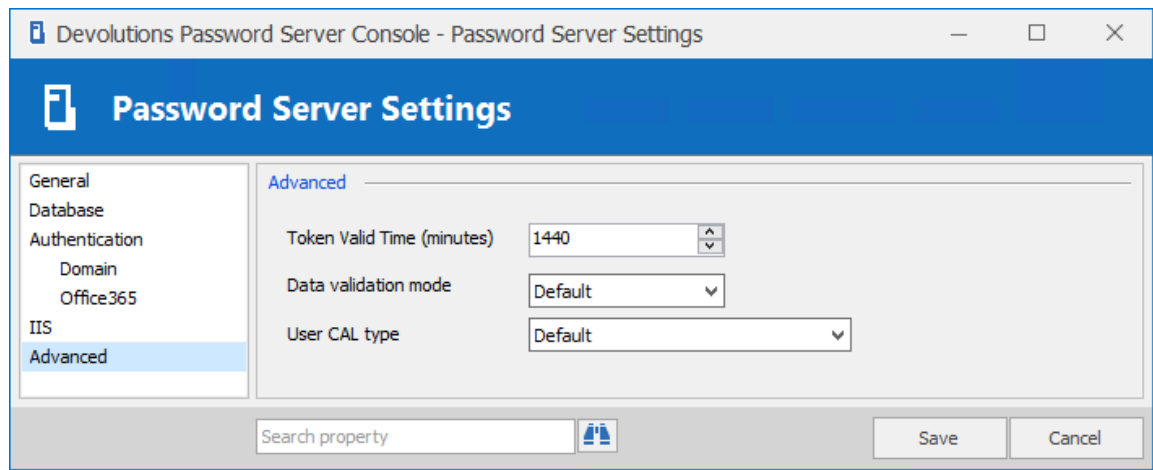
*IIS Manager HTTPS/SSL Dialog*

OPTION	DESCRIPTION
Certificate	Select the SSL Certificate will be use with the Devolutions Server instance.
Create Self-Signed Certificate...	Create a self-signed certificate to be use with the Devolutions Server instance.
Require SSL	The usage of a SSL certificate is mandatory when this option is enabled.

4.1.1.5 Advanced

DESCRIPTION

The Advanced tab permits to modify advanced settings in the Devolutions Server configuration.

*Advanced Tab*

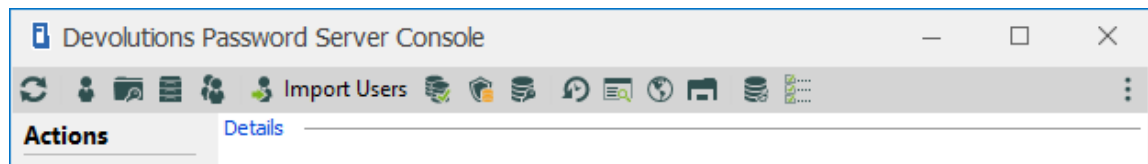
SETTINGS

CATEGORIE	DESCRIPTION
Token Valid Time (minutes)	This the duration time of the token. At the expiration of the token, the user must again authenticate himself on the Devolutions Server instance.
Data validation mode	Set the type of Date validation desired (Strict or Warning).
User CAL type	Choose which User license type the Devolutions Password Server instance will be use for between Connection Management and Password Management.

4.1.2 Commands

DESCRIPTION

The commands available on the toolbar of the Devolutions Password Server Console.



Devolutions Password Server Console Commands Toolbar

OPTION	DESCRIPTION
Refresh	Refresh the current information.
Manage Users	Manage users with the User Management .
Manage Security Groups	Opens the Security Group Management. (Legacy)
Manage Vaults	Opens the Vault Management .
Manage Roles	Opens the Role Management .
Import Users	Access the Import Users feature.
System Settings	Manage the System Settings .
System Permissions	Manage the System Permissions .
Security Providers	Manage the Security Providers .
Backup Manager	Access the Backup Manager feature.
View Logs	Access the View Logs feature.
View web client	Access the Web Interface .

OPTION	DESCRIPTION
Explore Content of web site directory	Uses File Explorer to Explore the website directory .
Pack Data Source	Access the Pack Data Source feature.
Options	Access the Options .

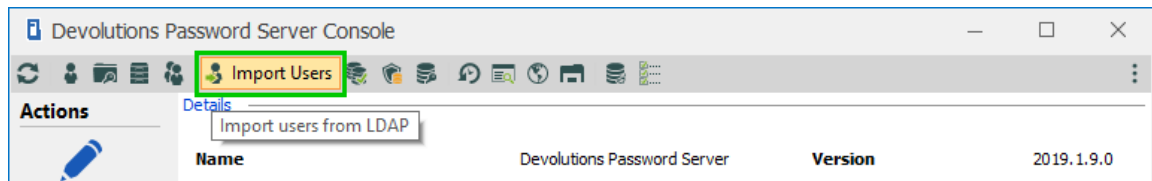
4.1.2.1 Import Users

DESCRIPTION



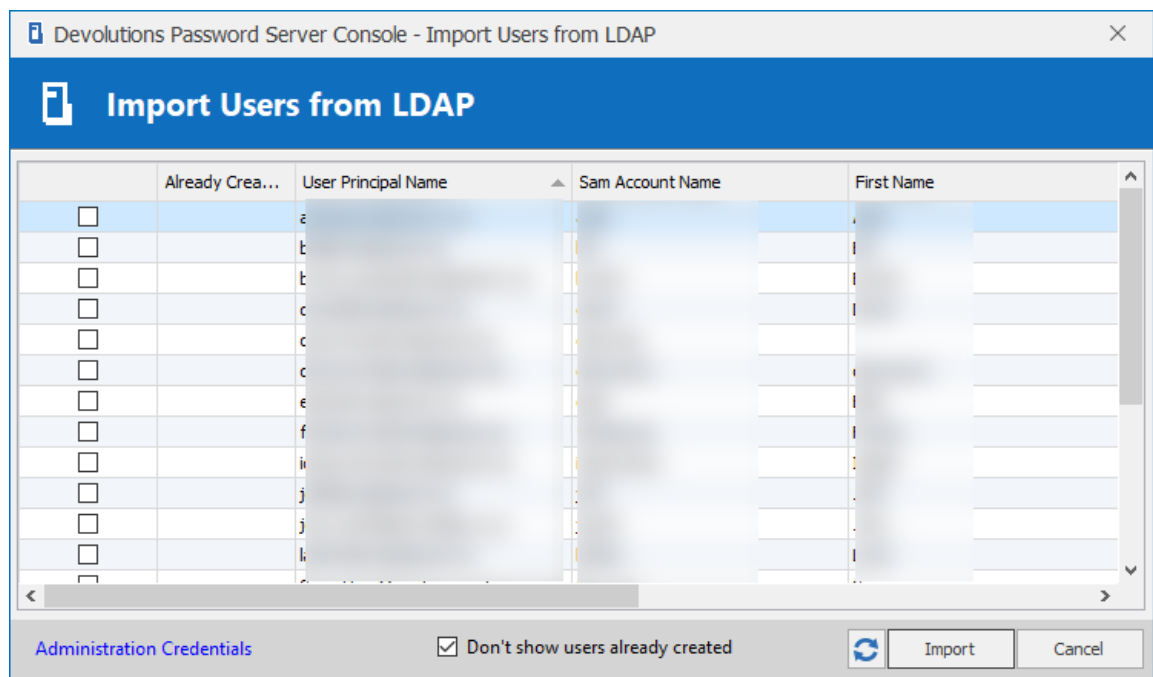
The Domain authentication method must be activated to be able to import users from LDAP. Consult the [Authentication](#) topic for more information.

From the Devolutions Password Server Console, click on the **Import Users** button.



Devolutions Password Server Console Commands Toolbar

Select the users you want to add and click on the **Import** button.



Import Users from LDAP Dialog

4.1.2.2 Backup Manager

DESCRIPTION

The **Backup Manager** is a feature that can create scheduled backups of the SQL database and the web configuration folder. It is also possible to create a live backup. The DevolutionsSchedulerService must be configured properly in order to work.

Start date/time	End date/time	N...	Filename	Database filename	Success
2018-08-02 9:22 AM	2018-08-02 9:23 AM	D...	\\Rigel\\Temp\\Web\\dvlsonion_02082018_132206...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-08-01 8:00 PM	2018-08-01 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_02082018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-07-31 8:00 PM	2018-07-31 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_01082018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-07-30 8:00 PM	2018-07-30 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_31072018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-07-29 8:00 PM	2018-07-29 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_30072018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-07-28 8:00 PM	2018-07-28 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_29072018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓
2018-07-27 8:00 PM	2018-07-27 8:01 PM	D...	\\Rigel\\Temp\\Web\\dvlsonion_28072018_130000...	\\DC\\TeamShare\\BackupDVLS\\Orion\\dvlsonion_...	✓

Backup Manager

For more information on the different options held in the Backup schedule settings please see:

- [Database](#)
- [Advanced](#)

For more information about the required account configuration please see:

- [Backup and restore Devolutions Server](#)

4.1.2.2.1 Database

DESCRIPTION

The following details the Database tab options of the **Backup Manager** feature.

Backup configuration

Database

Advanced

Database Configuration

Enable database backup☒

Backup database file path

\\PC\TeamShare\BackupDVLS

...

Web Configuration

Enable web backup☒

Backup database file path

\\PC\TeamShare\BackupDVLS

...

Schedule

Notify Administrator on backup failed☒

Backup start time

2018-06-01

9:20:00 PM

Repeat every

Days

1

Hours

0

Minutes

0

Save

Cancel

Backup Now

Start date/time	End date/time	N...	Filename	Database filename	Success
2018-08-02 9:22 AM	2018-08-02 9:23 AM	D...	\\Rigel\Temp\Web\dvlsorion_02082018_132206...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-08-01 8:00 PM	2018-08-01 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_02082018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-07-31 8:00 PM	2018-07-31 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_01082018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-07-30 8:00 PM	2018-07-30 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_31072018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-07-29 8:00 PM	2018-07-29 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_30072018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-07-28 8:00 PM	2018-07-28 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_29072018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓
2018-07-27 8:00 PM	2018-07-27 8:01 PM	D...	\\Rigel\Temp\Web\dvlsorion_28072018_130000...	\\PC\TeamShare\BackupDVLS\Orion\dvlsorion_...	✓

Backup Manager

SETTINGS

CONTROLS

BUTTON	DESCRIPTION
Save	Save the latest modifications of the Backup schedule options.
Cancel	Cancel the latest modifications of the Backup schedule options.
Backup Now	Create immediately a backup of the SQL database and/or the web application folder.

DATABASE CONFIGURATION

OPTION	DESCRIPTION
Enable database backup	Activate the backup of the SQL database.
Backup database file path	<p>The path to the folder where the backup of the SQL database will be saved. We recommend to use a shared network folder with proper permissions set on it to be able to save the backup file.</p> <p>Note: As the backup command is running on the SQL Server, this path must exist on the SQL Server or accessible from that SQL Server.</p>

WEB CONFIGURATION

OPTION	DESCRIPTION
Enable web backup	Activate the backup of the web application.
Backup web file path	The path to the folder where the backup of the web application will be saved. We recommend to use a shared network folder with proper permissions set on it to be able to save the backup file.

SCHEDULE

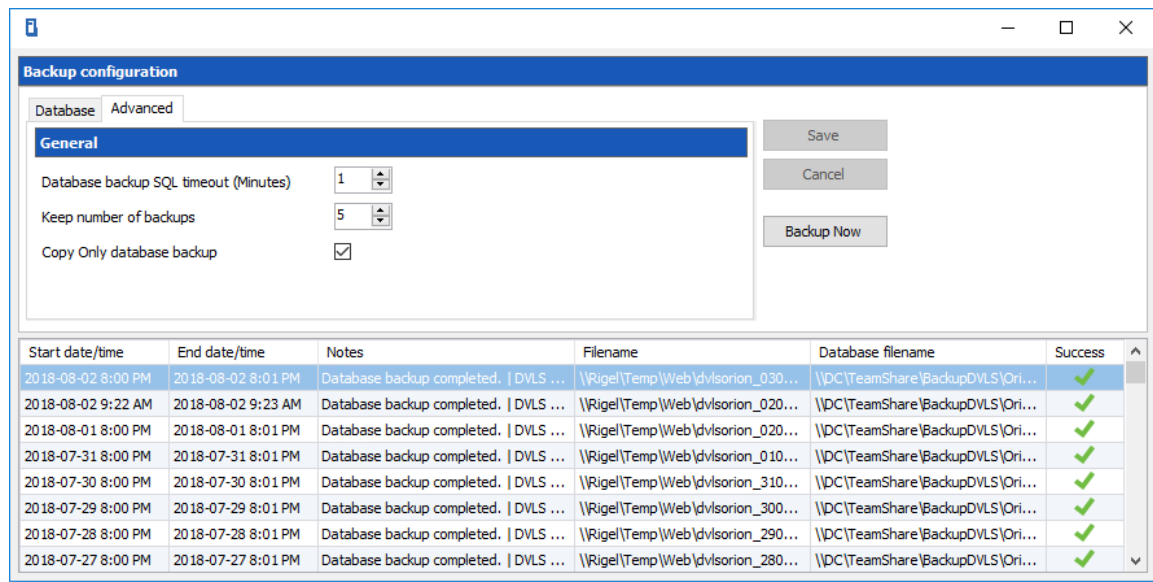
OPTION	DESCRIPTION
Notify Administrator on backup failed	Will send an email when the backup fails. The Email feature must be enabled in the Server Settings in order

OPTION	DESCRIPTION
	to work.
Backup start time	Date and time when the backup will be automatically started.
Repeat every	The time interval when the backup will be repeated.
Logs	<ul style="list-style-type: none">• Start date/time : The date and time when the backup was started.• End date/time : The date and time when the backup was finished.• Notes : Message to inform the completion or the fail of the backup.• Filename : Path and name of the web application backup file.• Database filename : Path and name of the SQL database backup file.• Success : Green check = successful; Red 'X' = fail.

4.1.2.2.2 Advanced

DESCRIPTION

The following details the Advanced tab options of the **Backup Manager** feature.



Backup Manager - Advanced

SETTINGS

GENERAL

OPTION	DESCRIPTION
Database backup SQL timeout (Minutes)	Number of minutes before a timeout in the SQL instance.
Keep number of backups	Number of the backup that will be kept in the backup folder.
Copy Only database backup	A SQL Server backup that is independent of the sequence of conventional SQL Server backups. For more information, please see https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/copy-only-backups-sql-server .

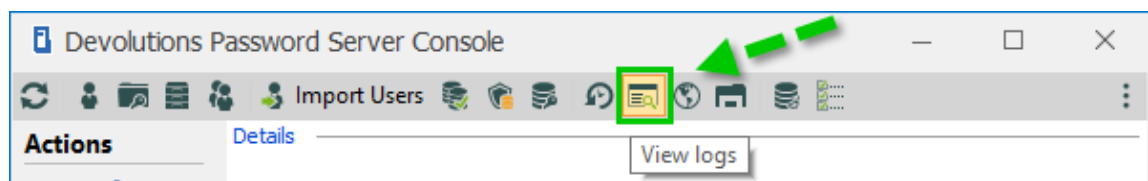
4.1.2.3 View logs

DESCRIPTION



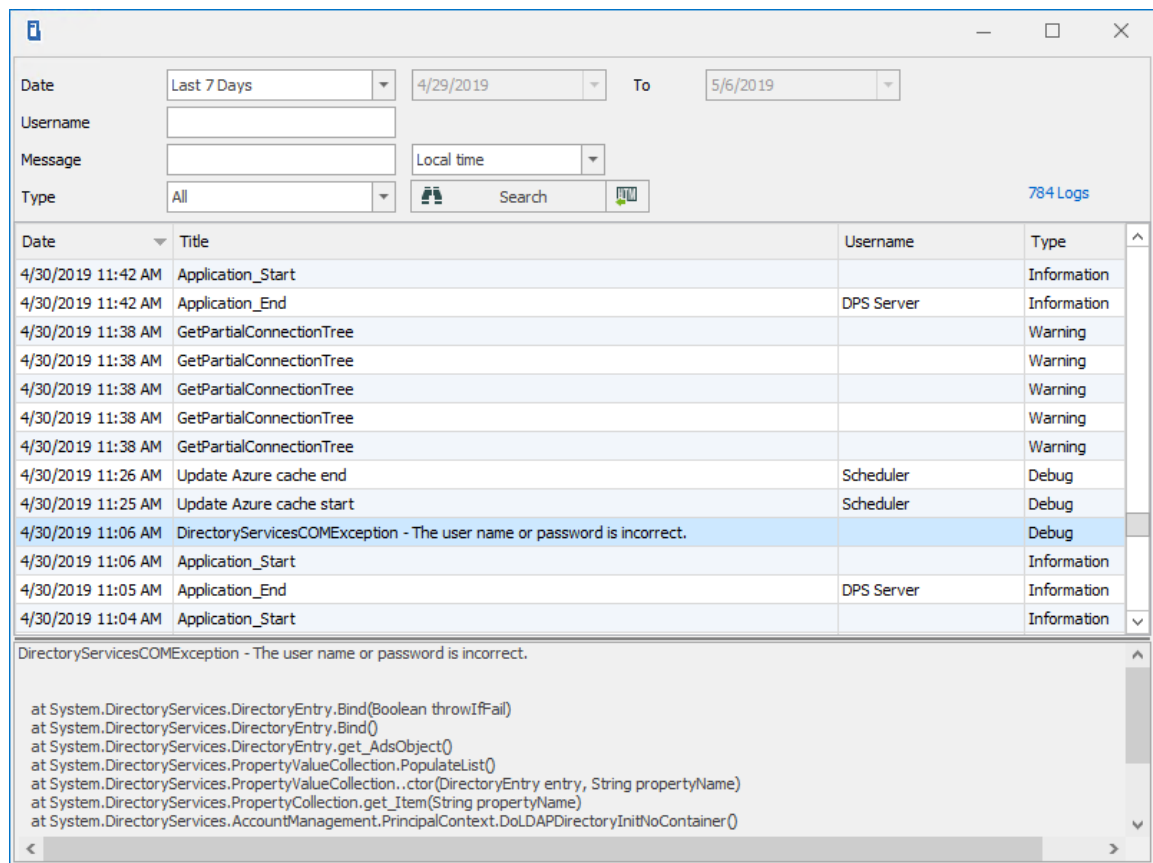
The Log debug information option must be enabled in order to view the logs. Consult the [Logging](#) topic for more information.

From the Devolutions Password Server Console, click on the **View logs** button.



Devolutions Password Server Console

Select the log entry to view the details in the bottom section.

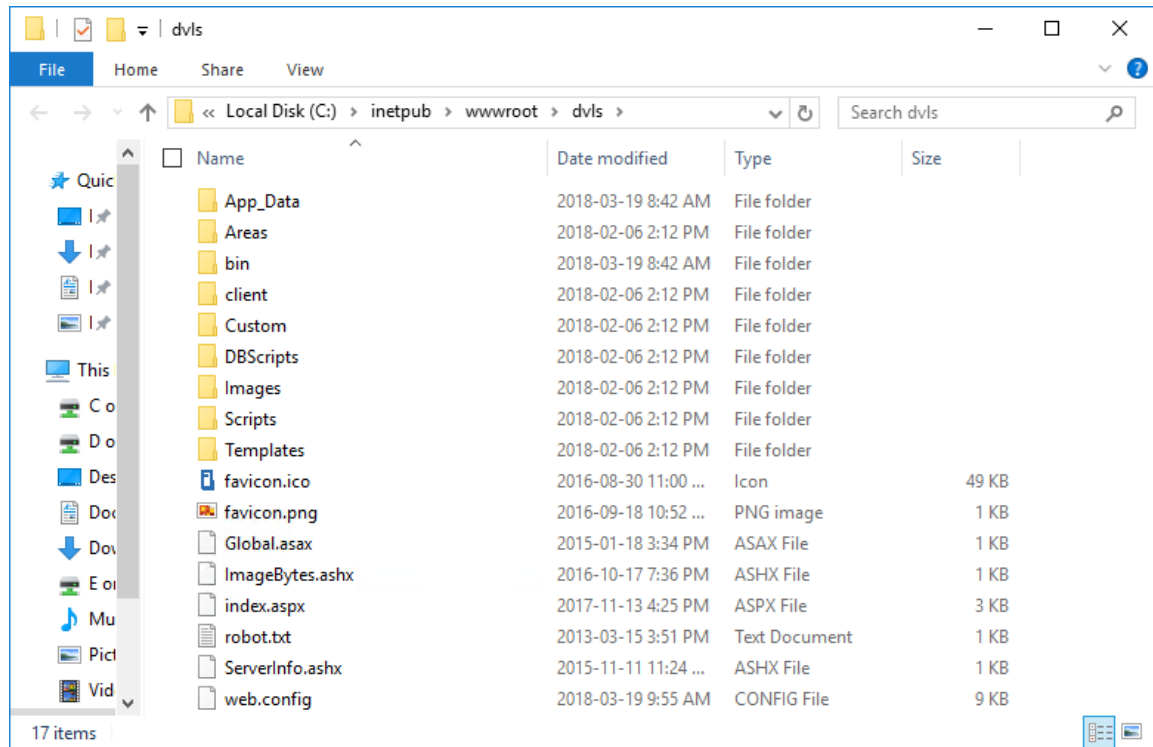


Devolutions Server Logs Dialog

4.1.2.4 Explore content of website directory

DESCRIPTION

The Explore content of website directory opens the Windows File Explorer in the folder where the Devolutions Server instance is located on the computer.



Web Site Folder

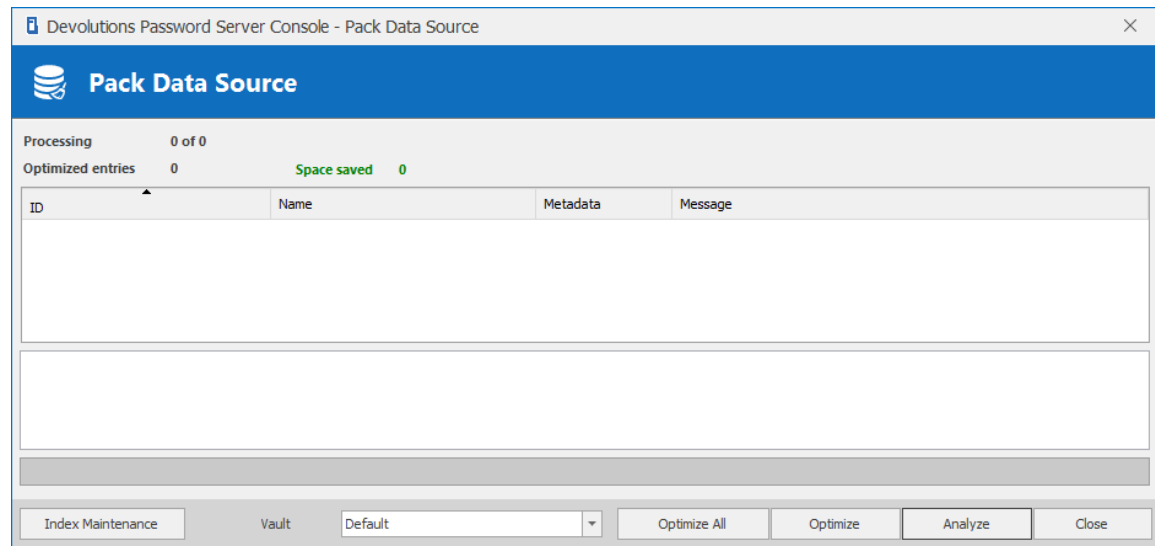
4.1.2.5 Pack Data Source

DESCRIPTION

When holding a great number of entries in your data source it is a best practice to compress them to avoid slowness issues when using your data source. The **Pack Data Source** will analyze all your entries, compress them and then resave them, thus saving space in your data source. With a Devolutions Server data source, the **Pack Data Source** tool is only be available through the Devolutions Password Server Console.



We recommend to backup your SQL database before performing **Index Maintenance** or **Optimize** operation.

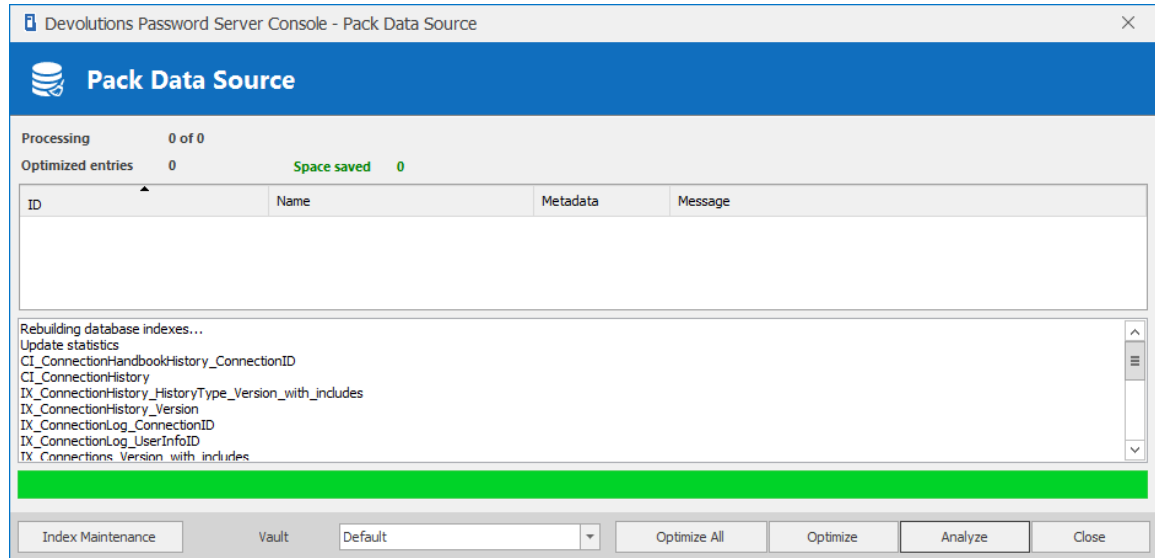


Pack Data Source Dialog

SETTINGS

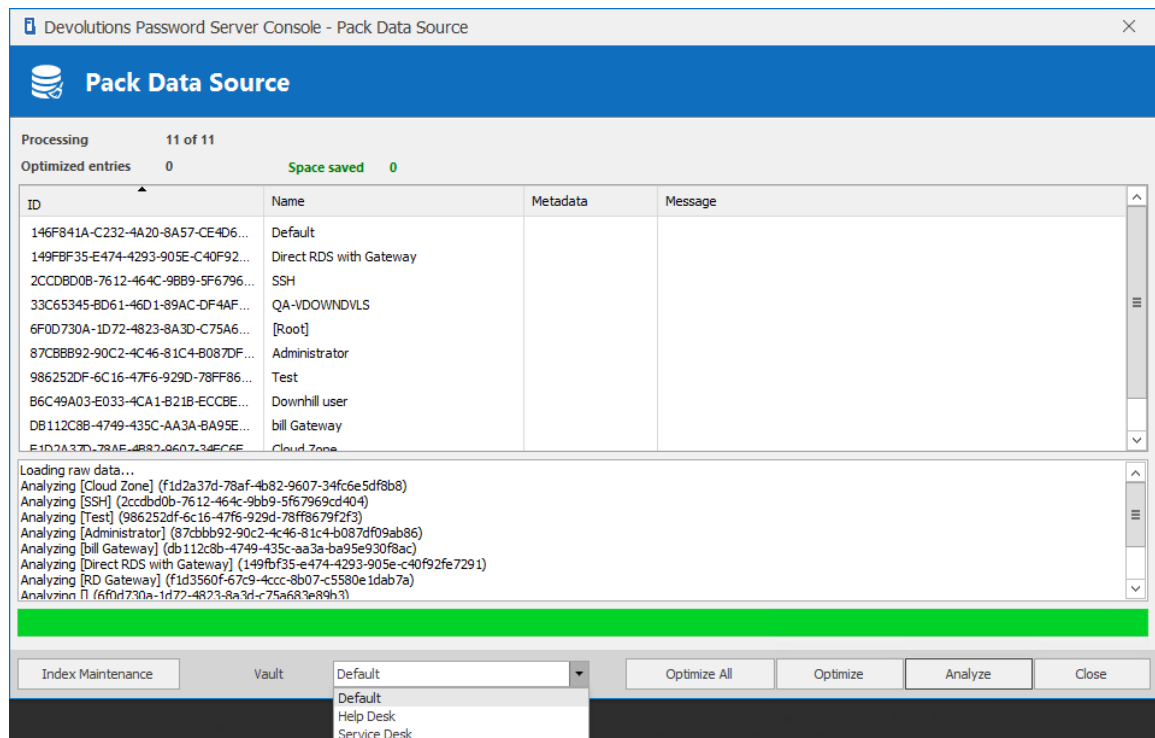
OPTION	DESCRIPTION
Index Maintenance	Will rebuild all database indexes.
Vault	Select on which Vault the Analyze or Optimize will be performed.
Optimize All	Will optimize all Vaults.
Optimize	Will optimize the data of the selected Vault. No needs to analyze the data before the optimize operation.
Analyze	Will analyze the content of all entries of the selected Vault and will produce a report of the amount of space that can be optimized.

INDEX MAINTENANCE



Index Maintenance - Pack Data Source Dialog

ANALYZE/OPTIMIZE

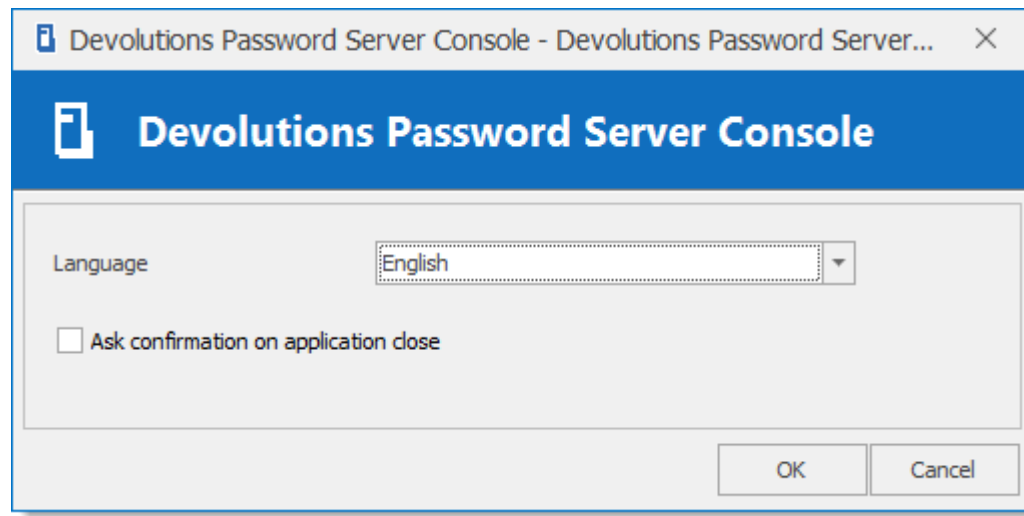


Analyze/Optimize - Pack Data Source Dialog

4.1.2.6 Options

DESCRIPTION

The Options command allows to modify the language of the Devolutions Password Server Console.



Options Dialog

SETTINGS

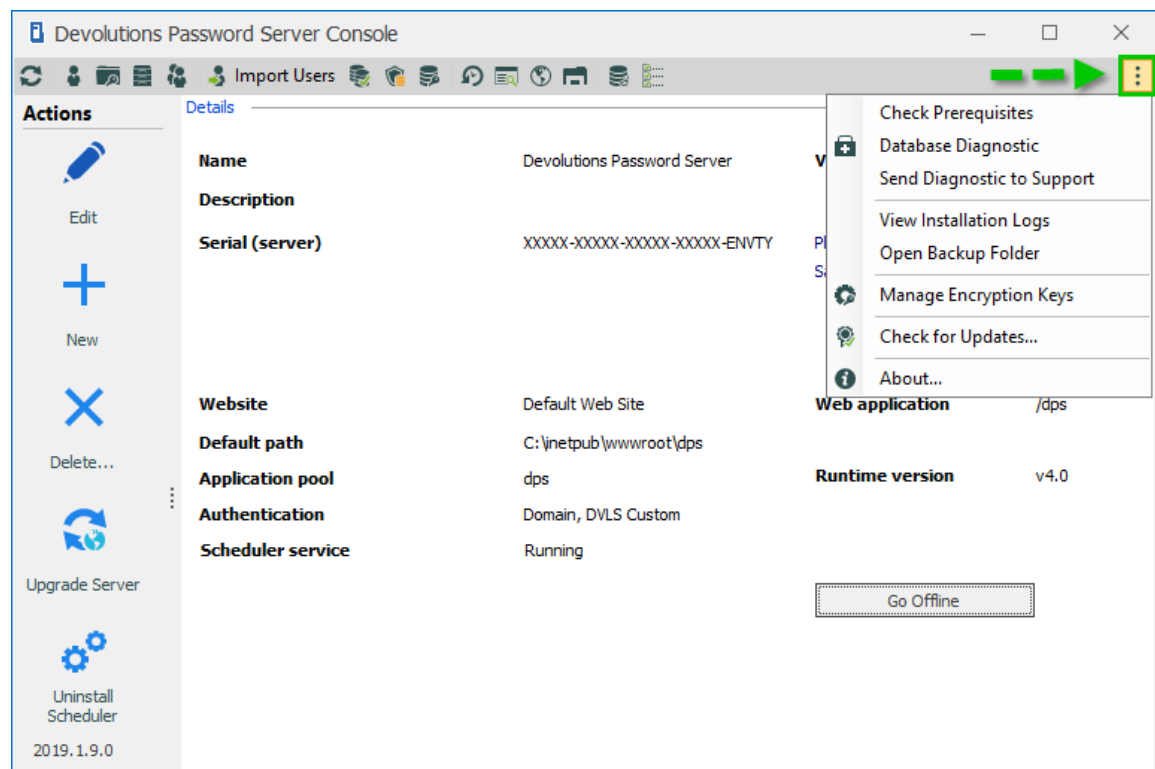
OPTION	DESCRIPTION
Language	<p>Select the language of the Devolutions Password Server Console.</p> <p>Language available :</p> <ul style="list-style-type: none">• English• Chinese (Simplified) Legacy• Chinese (Traditional, Taiwan)• Dutch• French

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• German• Italian• Polish (Poland)• Russian• Swedish (Sweden)• Ukrainian (Ukraine)
Ask confirmation on application close	Select on which Vault the Analyze or Optimize will be performed.

4.1.3 Advanced

DESCRIPTION

The **Advanced** menu offers tools available with Devolutions Server.

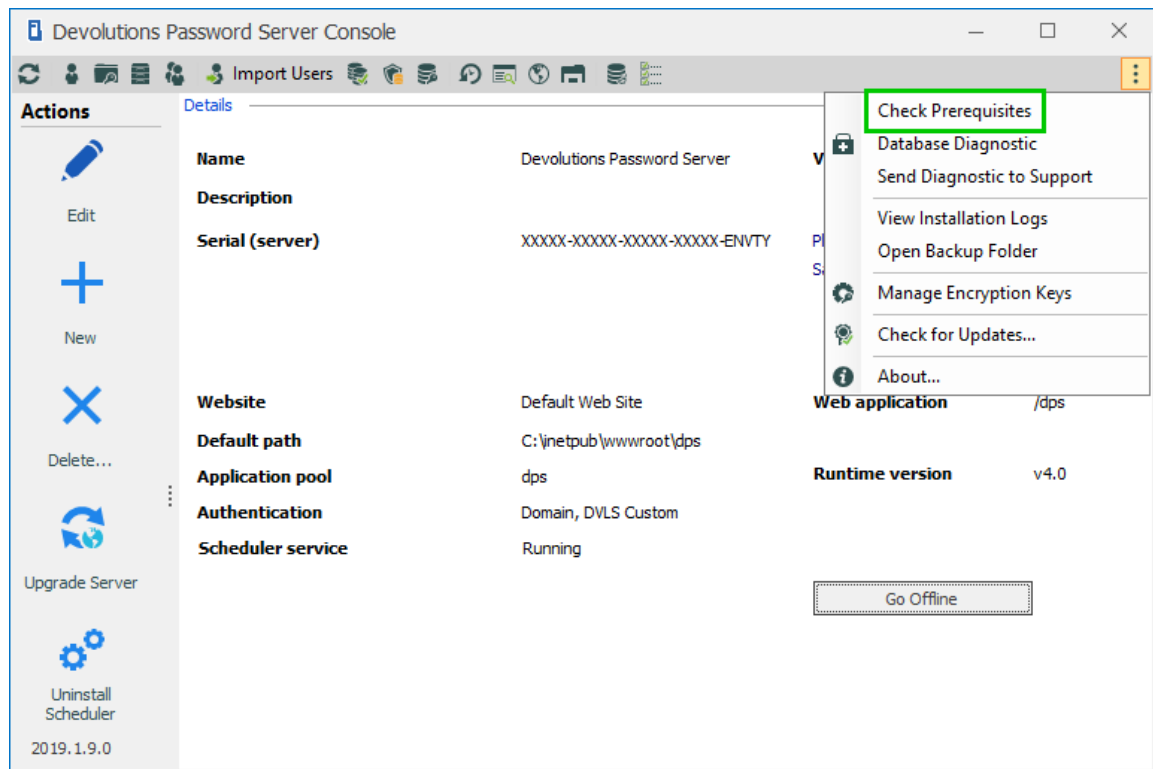
*Advanced Menu*

4.1.3.1 Check Prerequisites

DESCRIPTION

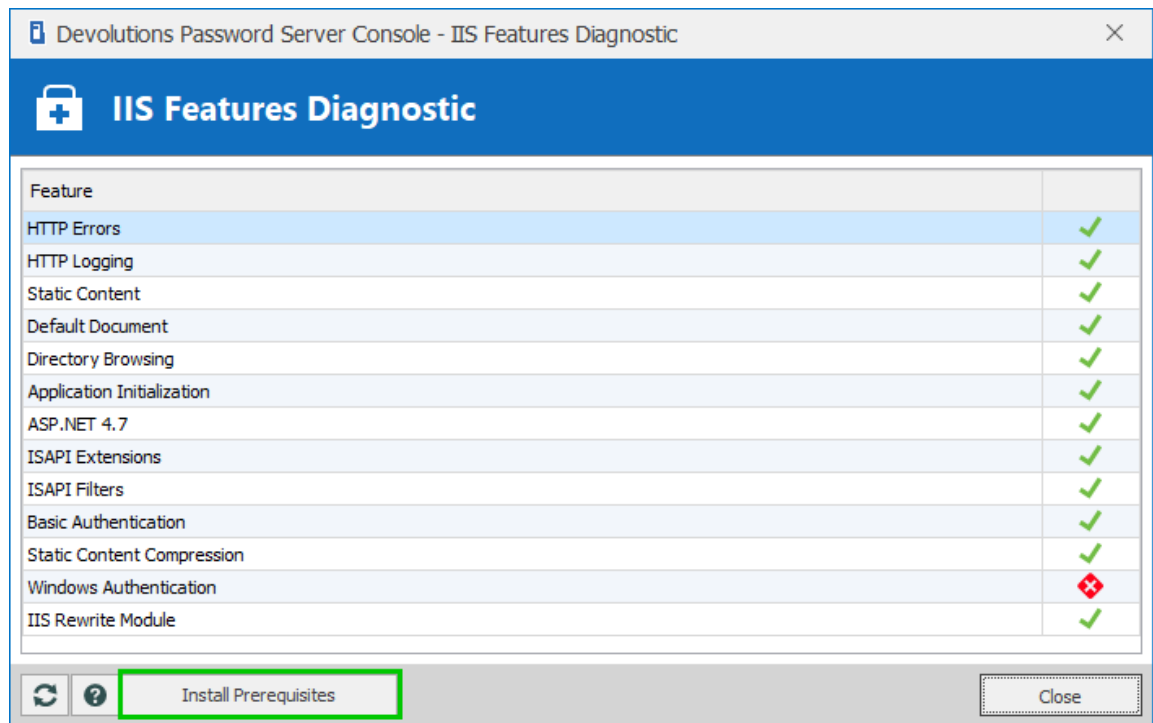
The **Check Prerequisites** validates if all the necessary IIS features are enabled to run Devolutions Server properly.

SETTINGS



Options Menu

This diagnostic will verify if all the IIS features are installed properly.



IIS Features Diagnostic

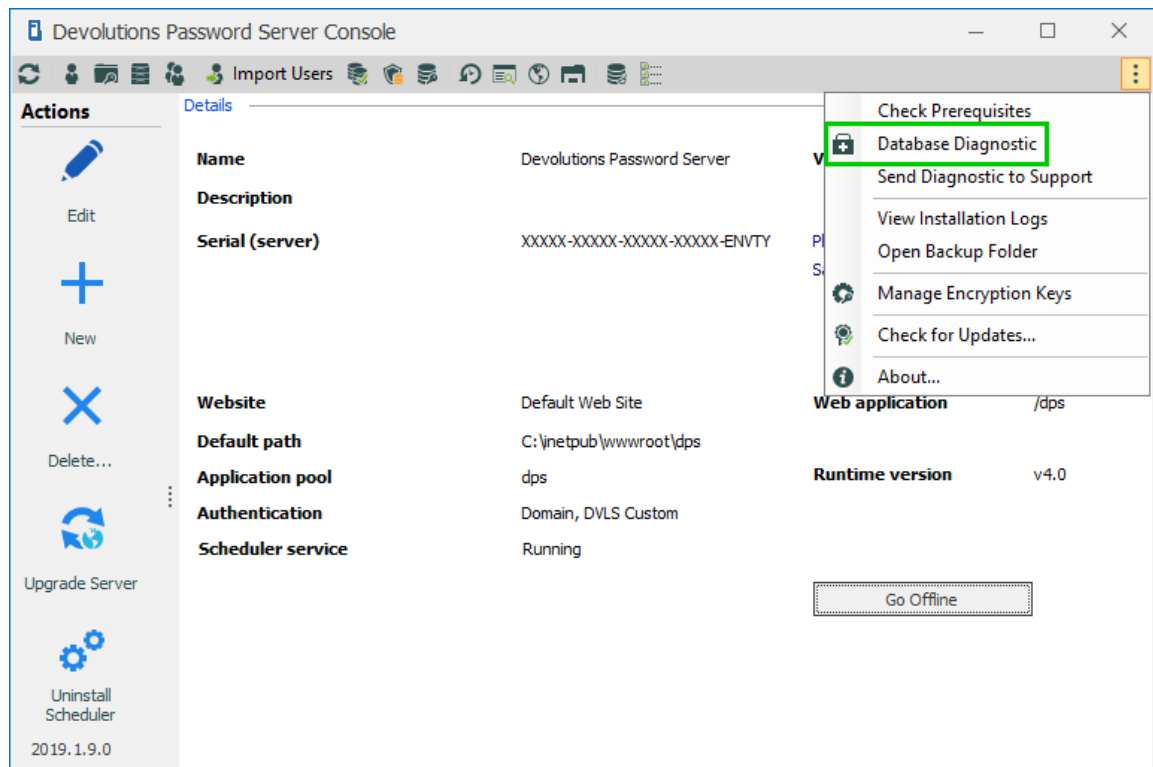
The **Install Prerequisites** button will run a PowerShell script to install the missing prerequisites. Please see [Installing Web Roles prerequisites](#).

4.1.3.2 Database Diagnostic

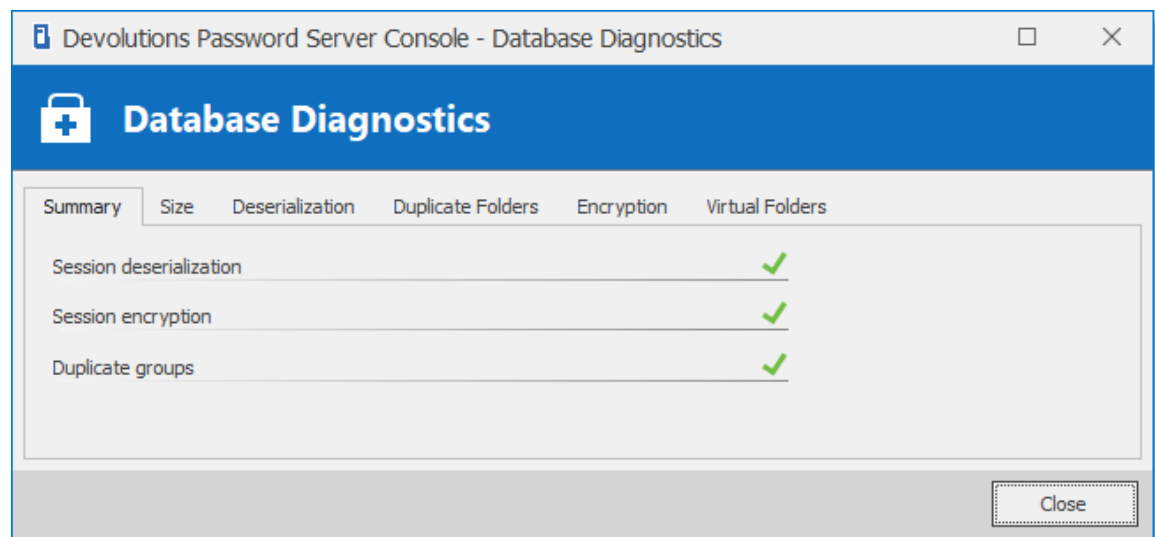
DESCRIPTION

The **Database Diagnostics** will display information of the database health. Please contact the support team at ticket@devolutions.net for more information about this report.

From the Devolutions Password Server Console, click on the ellipsis button on the right corner and select **Database Diagnostic**.



Advanced Menu



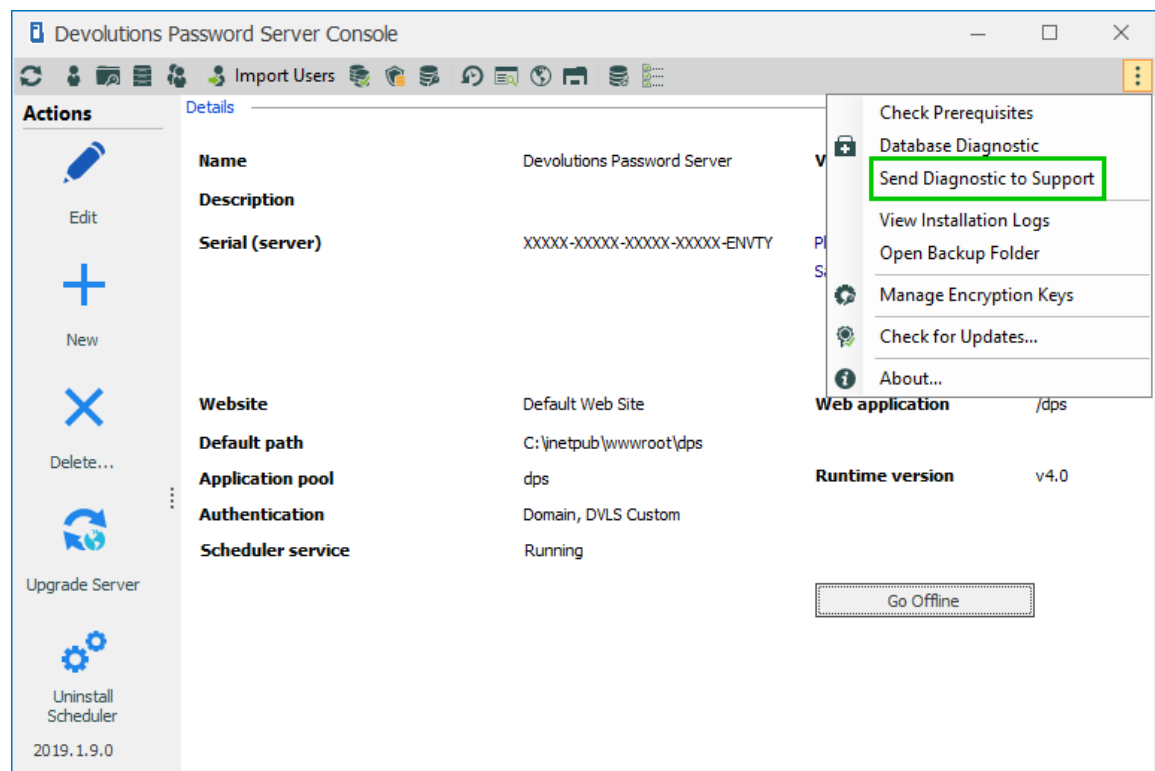
Database Diagnostic Dialog

4.1.3.3 Send Diagnostic to Support

DESCRIPTION

The **Send Diagnostic to Support** feature sends a diagnostic report that contains the configuration of the Devolutions Server to our support team.

From the Devolutions Password Server Console, click on the ellipsis button on the right corner and select **Send Diagnostic to Support**.

*Advanced Menu*

Fill in the field and click on the **OK** button.

Devolutions Password Server Console - Send Message to Devolutions Support Team

Send Message to Devolutions Support Team

Personal Information

Email: YourEmail@YourDomain.com

Company: Your Company

Name: Your Name Here

Subject:

Message

Save to File OK Cancel

Send Diagnostic Report Dialog

SETTINGS

OPTION	DESCRIPTION
Email	Write in your email address.
Company	Write in your company name.
Name	Write in your full name.
Subject	Write in a subject line for the report.
Message	Add any further details in the message box.

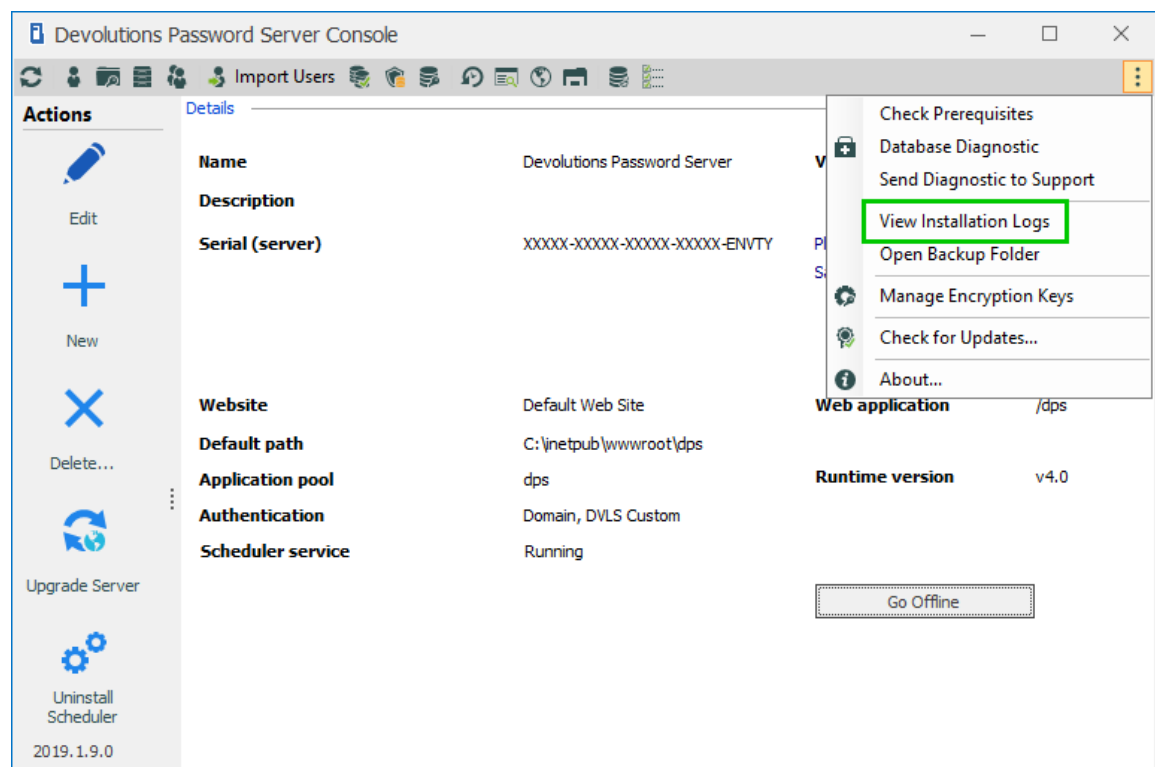
OPTION	DESCRIPTION
Save to File	Save the diagnostic report in a text file. Useful when the computer doesn't have internet access.

4.1.3.4 View Installation Logs

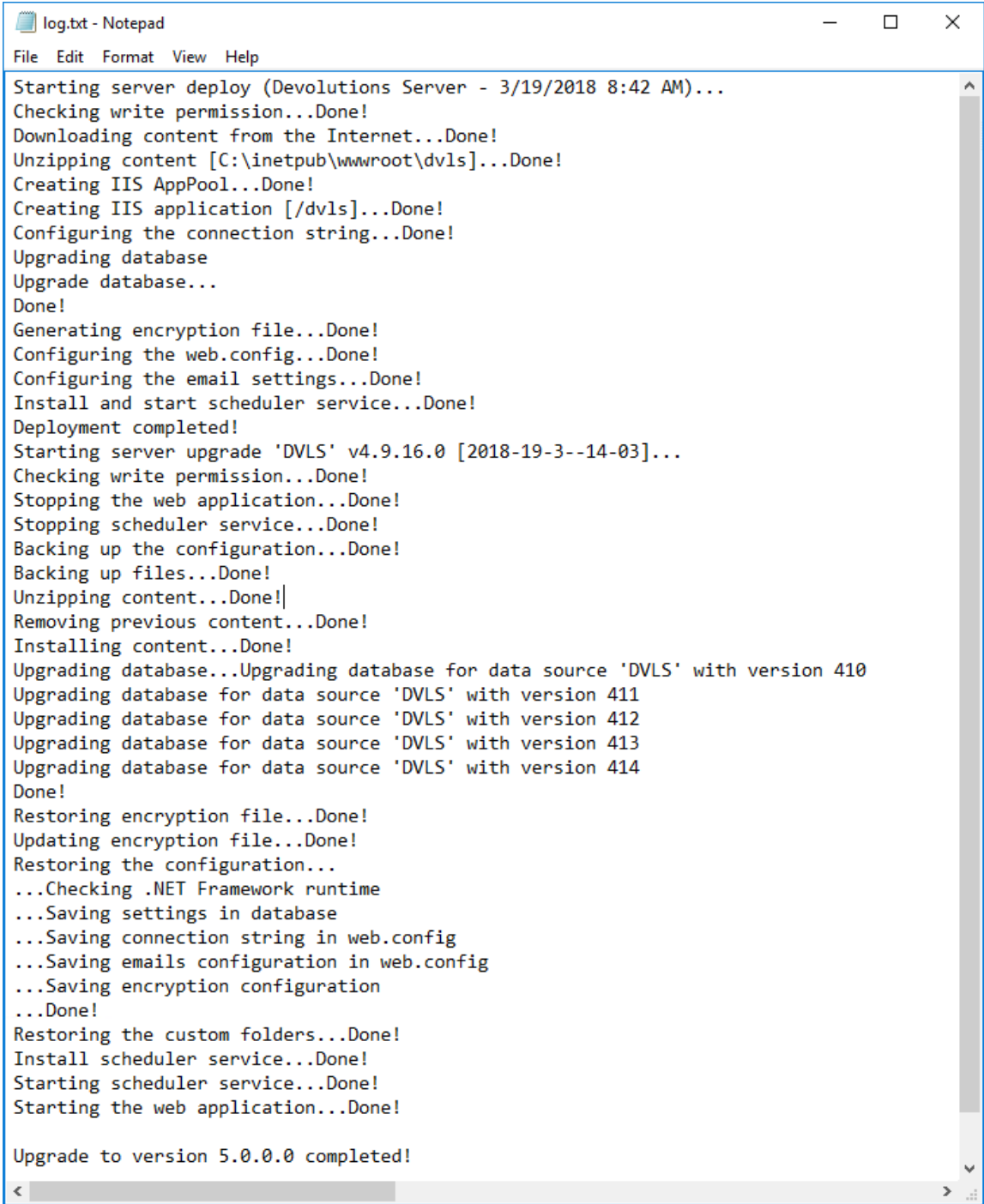
DESCRIPTION

This will open the **log.txt** file that includes the steps of the installation/upgrade process. This file will grow along the different upgrades of the Devolutions Server instance.

From the Devolutions Password Server Console, click on the ellipsis button on the right corner and select **View Installation Logs**.



Advanced Menu



```
log.txt - Notepad
File Edit Format View Help

Starting server deploy (Devolutions Server - 3/19/2018 8:42 AM)...
Checking write permission...Done!
Downloading content from the Internet...Done!
Unzipping content [C:\inetpub\wwwroot\dvls]...Done!
Creating IIS AppPool...Done!
Creating IIS application [/dvls]...Done!
Configuring the connection string...Done!
Upgrading database
Upgrade database...
Done!
Generating encryption file...Done!
Configuring the web.config...Done!
Configuring the email settings...Done!
Install and start scheduler service...Done!
Deployment completed!
Starting server upgrade 'DVLS' v4.9.16.0 [2018-19-3--14-03]...
Checking write permission...Done!
Stopping the web application...Done!
Stopping scheduler service...Done!
Backing up the configuration...Done!
Backing up files...Done!
Unzipping content...Done!
Removing previous content...Done!
Installing content...Done!
Upgrading database...Upgrading database for data source 'DVLS' with version 410
Upgrading database for data source 'DVLS' with version 411
Upgrading database for data source 'DVLS' with version 412
Upgrading database for data source 'DVLS' with version 413
Upgrading database for data source 'DVLS' with version 414
Done!
Restoring encryption file...Done!
Updating encryption file...Done!
Restoring the configuration...
...Checking .NET Framework runtime
...Saving settings in database
...Saving connection string in web.config
...Saving emails configuration in web.config
...Saving encryption configuration
...Done!
Restoring the custom folders...Done!
Install scheduler service...Done!
Starting scheduler service...Done!
Starting the web application...Done!

Upgrade to version 5.0.0.0 completed!
```

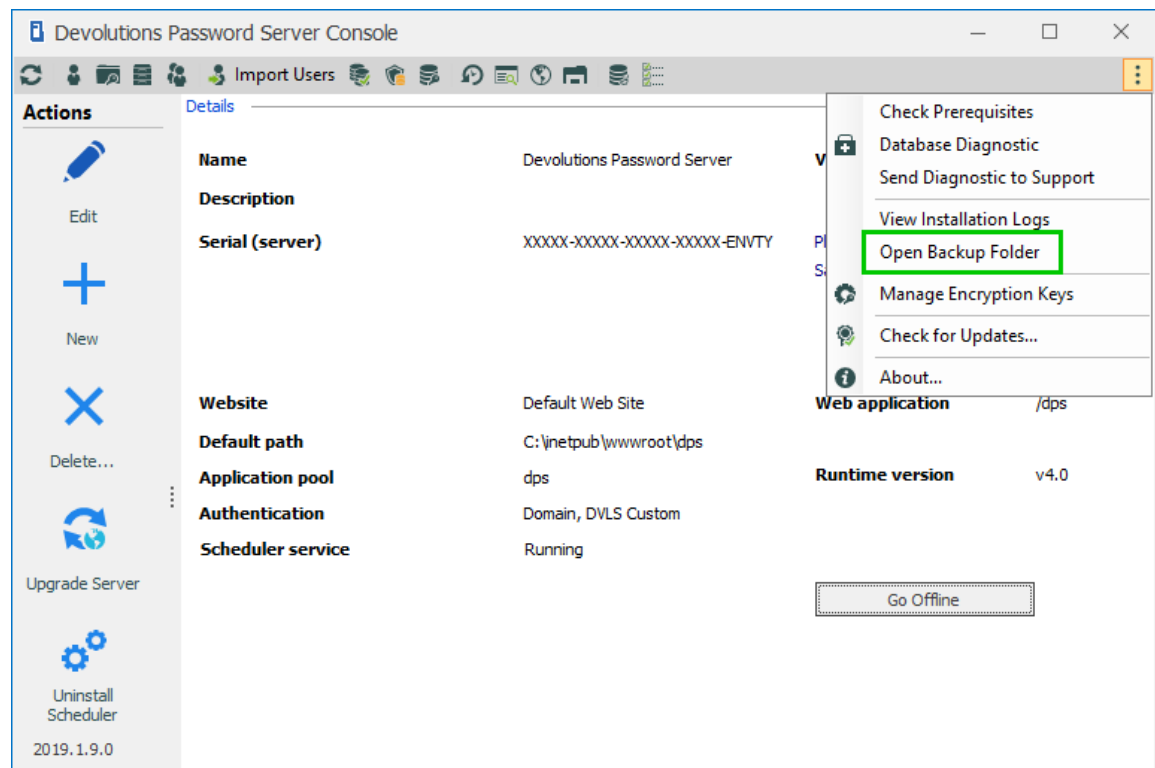
Installation/Upgrade Logs File

4.1.3.5 Open Backup Folder

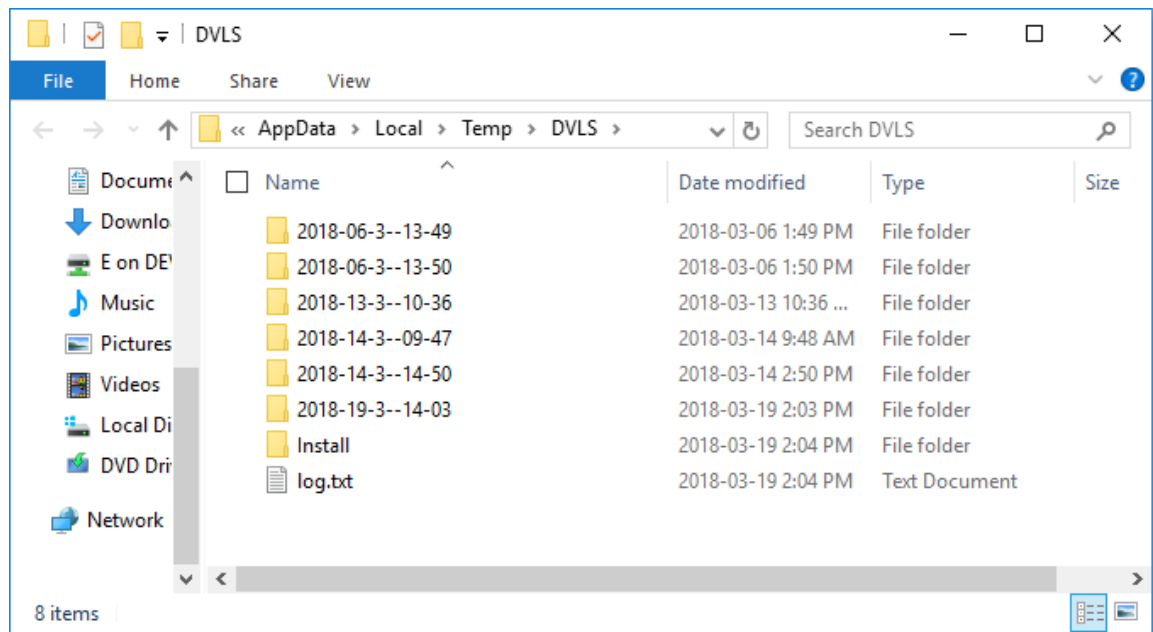
DESCRIPTION

It will open the Windows File Explorer in the folder where the backup of the Devolutions Password Server instance was saved during the upgrade process. The DVLS folder is normally located in **%LOCALAPPDATA%\Temp**.

From the Devolutions Password Server Console, click on the ellipsis button on the right corner and select **Open Backup Folder**.



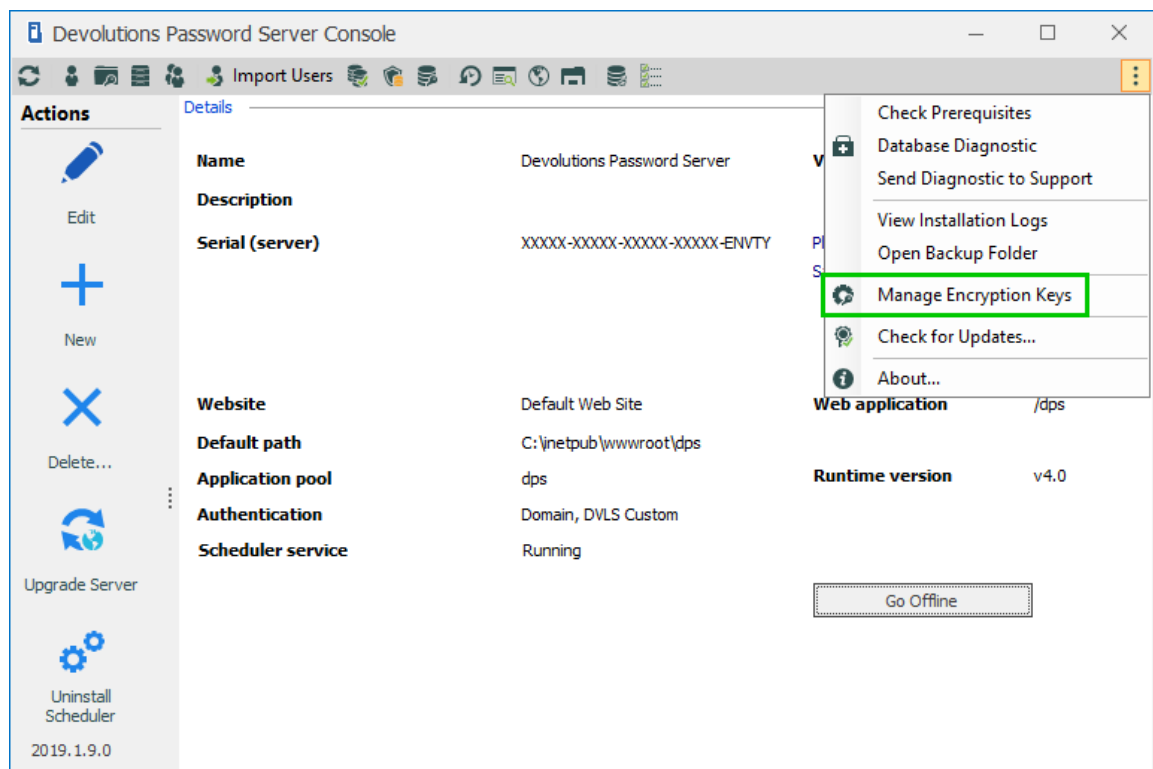
Advanced Menu

*Backup Folder*

4.1.3.6 Manage Encryption Keys

DESCRIPTION

From this dialog, it is possible to manage the different encryption keys used by Devolutions Server.

*Advanced Menu**Manage Encryption Keys Dialog*

SETTINGS



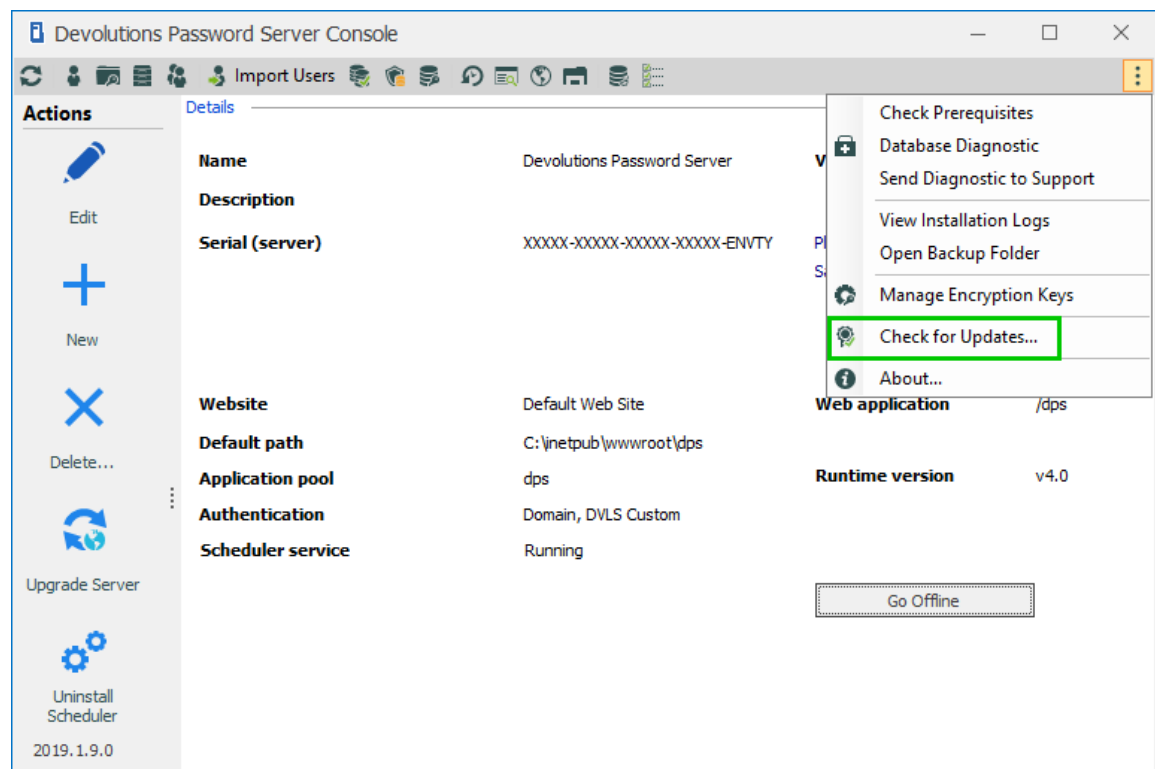
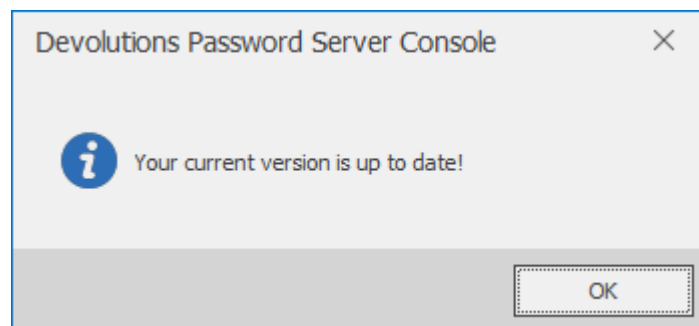
Importing or regenerate will encrypt the data in the SQL database. Be sure to backup the SQL database before. If the Devolutions Server is deployed in a High Availability or Load Balancing topology, the encryption keys must be the same on all Devolutions Server instances connected on the same SQL database.

OPTION	DESCRIPTION
Operation	<ul style="list-style-type: none">• Export : Allows to export the encryption keys in a .bin file.• Import : Allows to import the encryption keys from a .bin file.• Regenerate : Allows to regenerate the encryption keys.
Login Key	The encrypted key used by Devolutions Server for logins.
Token Storage Key	The encrypted key used by Devolutions Server for the token.
Security provider configuration	The encrypted key used by Devolutions Server for the Security Provider configuration.
Password	The password required to export the encryption keys into a file or import them from a file.

4.1.3.7 Check for Updates

DESCRIPTION

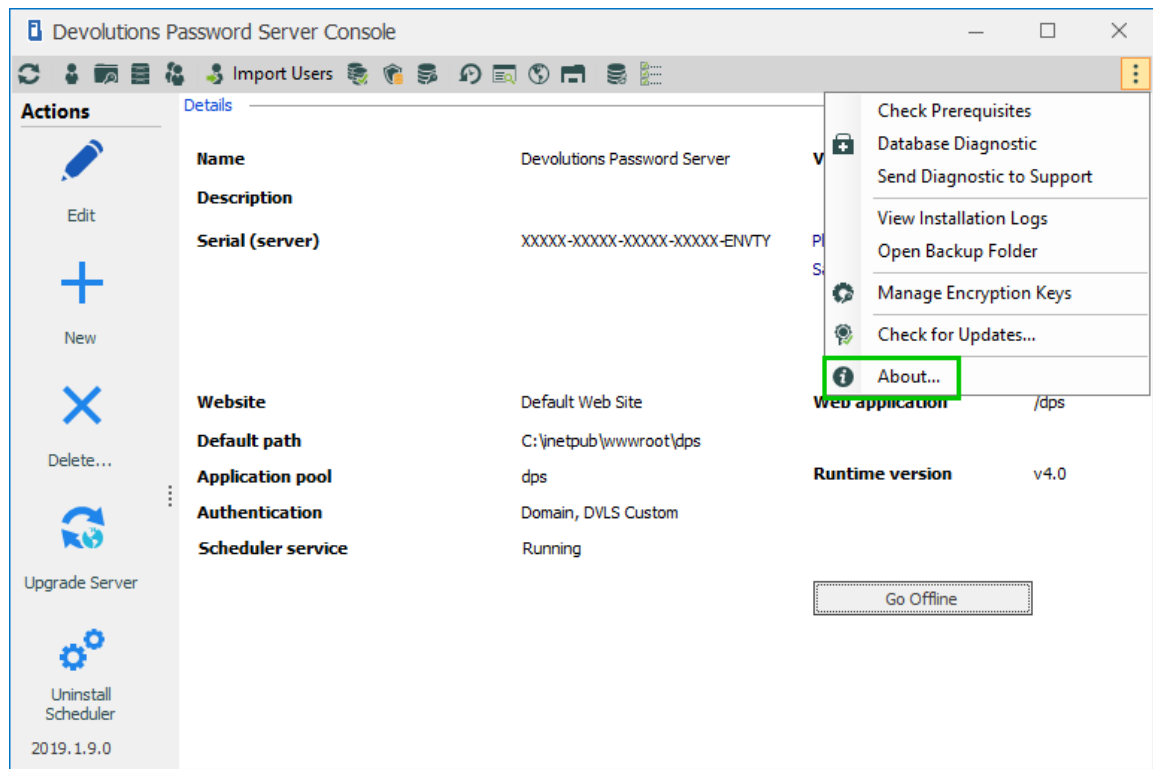
Will check if the Devolutions Password Server Console version is up to date.

*Advanced Menu**Check for Updates Dialog*

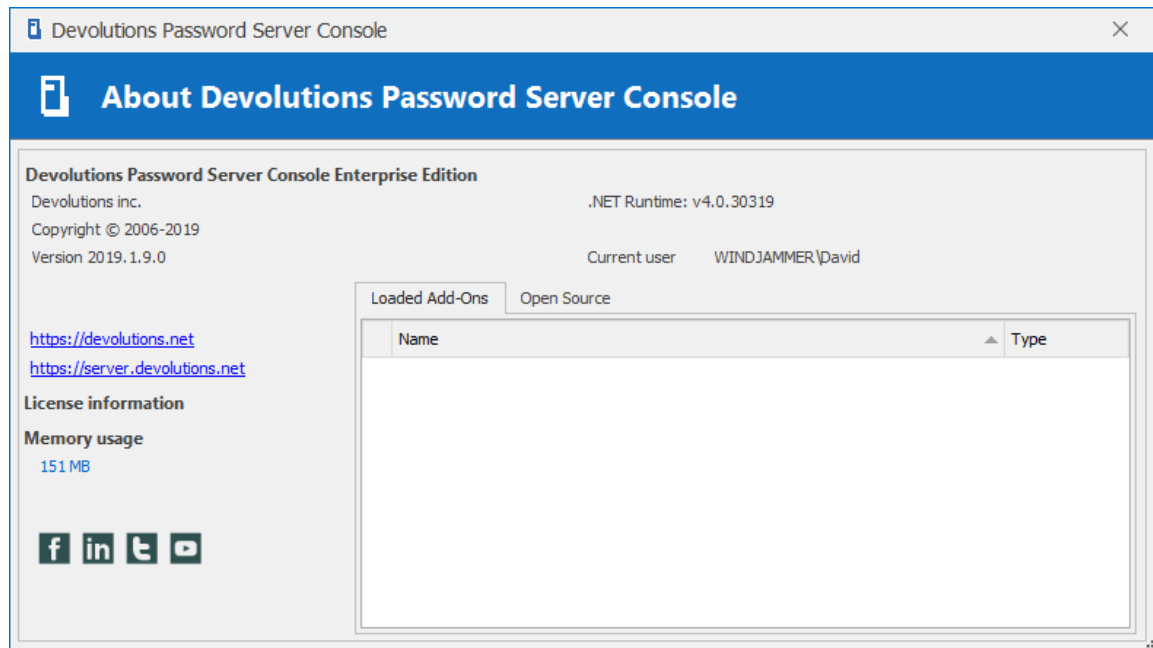
4.1.3.8 About

DESCRIPTION

Will display the current **About** dialog that contains the Devolutions Password Server Console version and some other information about the current machine.



Advanced Menu

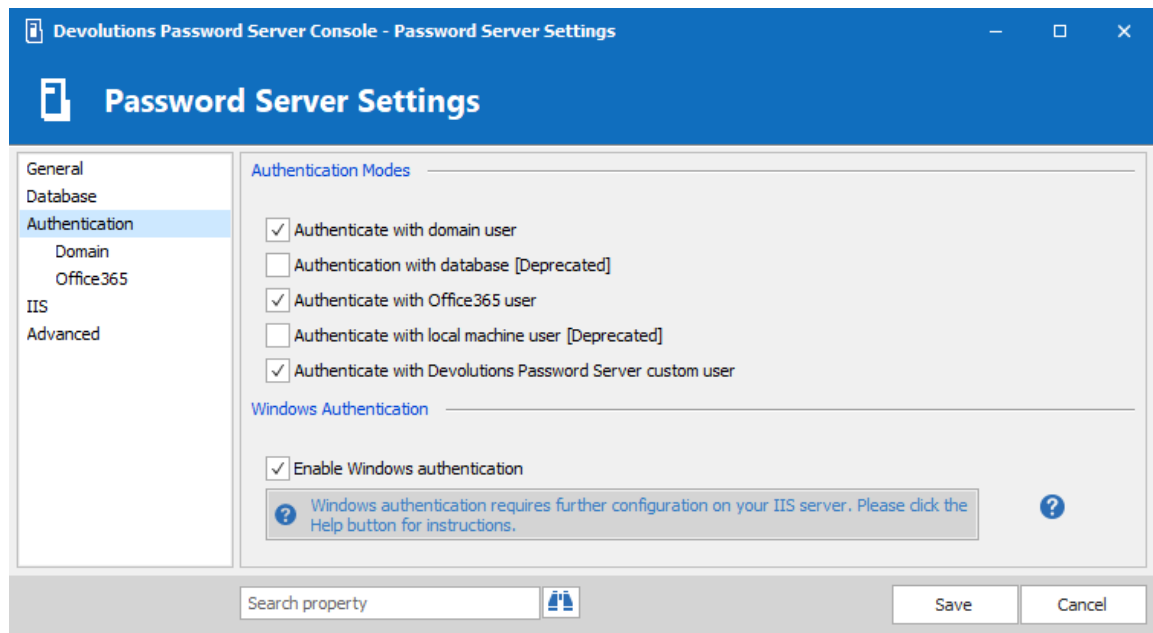


About Dialog

4.2 Authentication

DESCRIPTION

Devolutions Server supports multiple authentication modes.



Authentication Tab

SETTINGS

AUTHENTICATION MODES

OPTION	DESCRIPTION
Authenticate with domain user	The domain is used to authenticate the user.
Authenticate with database user	The database is used to authenticate the user. This authentication method is now identified as deprecated.
Authenticate with Office365 user	AzureAD is used to authenticate the user.

OPTION	DESCRIPTION
Authenticate with local machine user	The application allows a local user to be authenticated on the server. This authentication method is now identified as deprecated.
Authenticate with Devolutions Server custom user	The Devolutions Server is used to authenticate the user. You must create the initial user through the console.

WINDOWS AUTHENTICATION

OPTION	DESCRIPTION
Enable Windows Authentication	The application will use the current Windows authenticated user to authenticate to the Devolutions Server instance.

AUTOMATIC USER ACCOUNT CREATION

When using authentication modes other than **Active Directory**, user accounts must be created beforehand in order to grant access to the system.

When you are using **Active Directory** authentication, two choices are offered to you:

1. Create the user accounts manually, just as with the other authentication modes

or

2. Enable **Automatic Account Creation**, and let Devolutions Server create user accounts as soon as they are authenticated by the domain the instance is linked to.

After the account is created, rights and permissions are assigned either manually to the user account, or through membership in AD groups for which you have created a role mapping.



User accounts created by the server have no rights other than logging on the system. They will be able to see and edit the resources that have **no security** defined. You must ensure that all entries are protected. This is achieved easily by setting all permissions of the [Root Settings](#) to **Never**.

Depending on the authentication mode used, the username may be prefixed by the domain name, and the exact naming convention is controlled by the domain. For instance, for a **WINDJAMMER** domain that is registered as **windjammer.loc**, we have no way of knowing beforehand what form will be reported by the AD services. It is recommended to always enable both Devolutions Server authentication initially and create an Administrator account for the initial phase of implementation.

4.3 Security

DESCRIPTION

The **Security** section of the Devolutions Password Server Console allows you to manage your instance. These management features are exactly the same as the one offered under the **Administration** tab of the various Desktop Clients (such as Remote Desktop Manager), **when they are connected to that instance through a Data source**.

Since the latter is the one you will spend most of your time using, whenever a new instance is created, we recommend creating an administrative user, then register the instance as a data source in your Desktop Client of choice. This will bring you in a more familiar territory and will help you get around more quickly.

If you are indeed using full AD integration, whereas the assignment of permissions comes mostly from AD Group membership, then the roles are the mechanism that make this work.

The sections below are to cover the basic management features if you cannot use a desktop client.

- [User Management](#)
- [Role Management](#)
- [Vault Management](#)

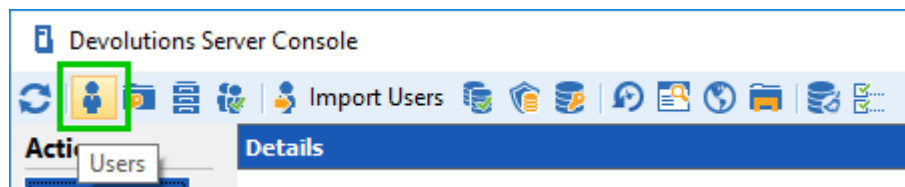
4.3.1 User Management

DESCRIPTION

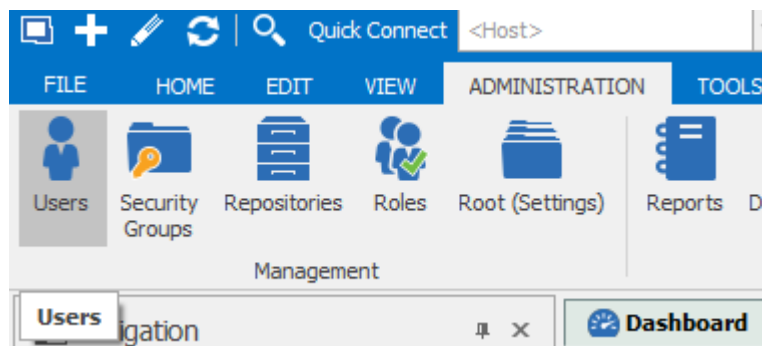


In order to create users and assign rights, you must be administrator of not only Devolutions Server, but also of the underlying database.

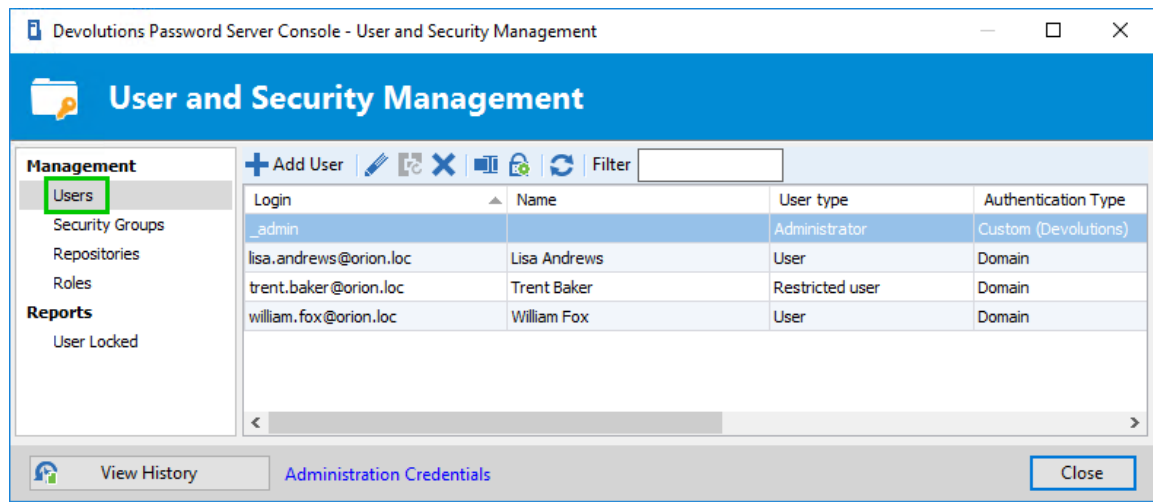
The **User Management** is available from **Administration - Users** within Remote Desktop Manager or on the toolbar of the Devolutions Password Server Console. **User Management** allows you to create and manage users and their permissions. Devolutions Server offers advanced user rights management that allows for restricting access to entries. Please note that some features availability depends on the active data source.



Manage Users in Devolutions Password Server Console



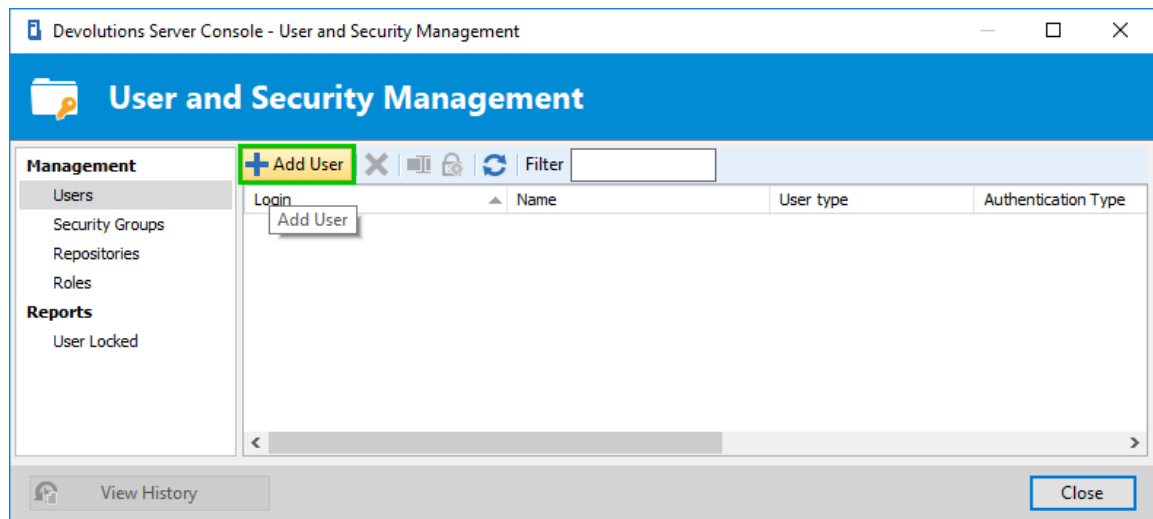
Manage Users in Remote Desktop Manager

*Users Management Dialog*

SETTINGS

CREATE USERS

To create a new user in your data source click on **Add User**.

*User Management - Add User*

USER MANAGEMENT SETTINGS

GENERAL

The screenshot shows the 'User Management' window in the Devolutions Password Server Console. The window has a blue header with a user icon and the title 'User Management'. On the left is a sidebar with a tree view containing: General (selected), Information, Roles, Privileges, Security Groups, Vaults, Application Access, Settings, and Email Notifications. The main area is divided into two sections: 'General' and 'Information'. The 'General' section contains fields for ID (5C68ADAB-F8BE-42F5-A791-697844D4DD85), Authentication type (Custom (Devolutions)), Username, Password, User type (User), User license type (Default), and checkboxes for 'Enabled' (checked), 'User must change password at next logon', and 'Send user an email invite'. The 'Information' section contains fields for First name, Last name, and Email. At the bottom right are 'OK' and 'Cancel' buttons.

User Management - General

OPTION	DESCRIPTION
Authentication type	<p>Select the user's authentication type:</p> <ul style="list-style-type: none"> • Custom (Devolutions): create a user specific to Devolutions Server without creating an SQL login. • Domain : authenticate using the Active Directory user account. • Database (SQL Server): authenticate using the SQL login from your SQL Server.
Username	Enter the login name for the user.

OPTION	DESCRIPTION
Password	Enter the user's Password. This field is only enable using Custom (Devolutions).
User type	Select the type of user to create: Select between: <ul style="list-style-type: none">• Administrator: grant full administrative rights to the user.• Read only user: grant only the View access to the user.• Restricted user: select which rights to grant to the user.• User: grant all basic rights to the user (Add, Edit, Delete).
First and Last name	Displays the First name and Last name of the Information tab.
Email	Insert the user's email address.

INFORMATION

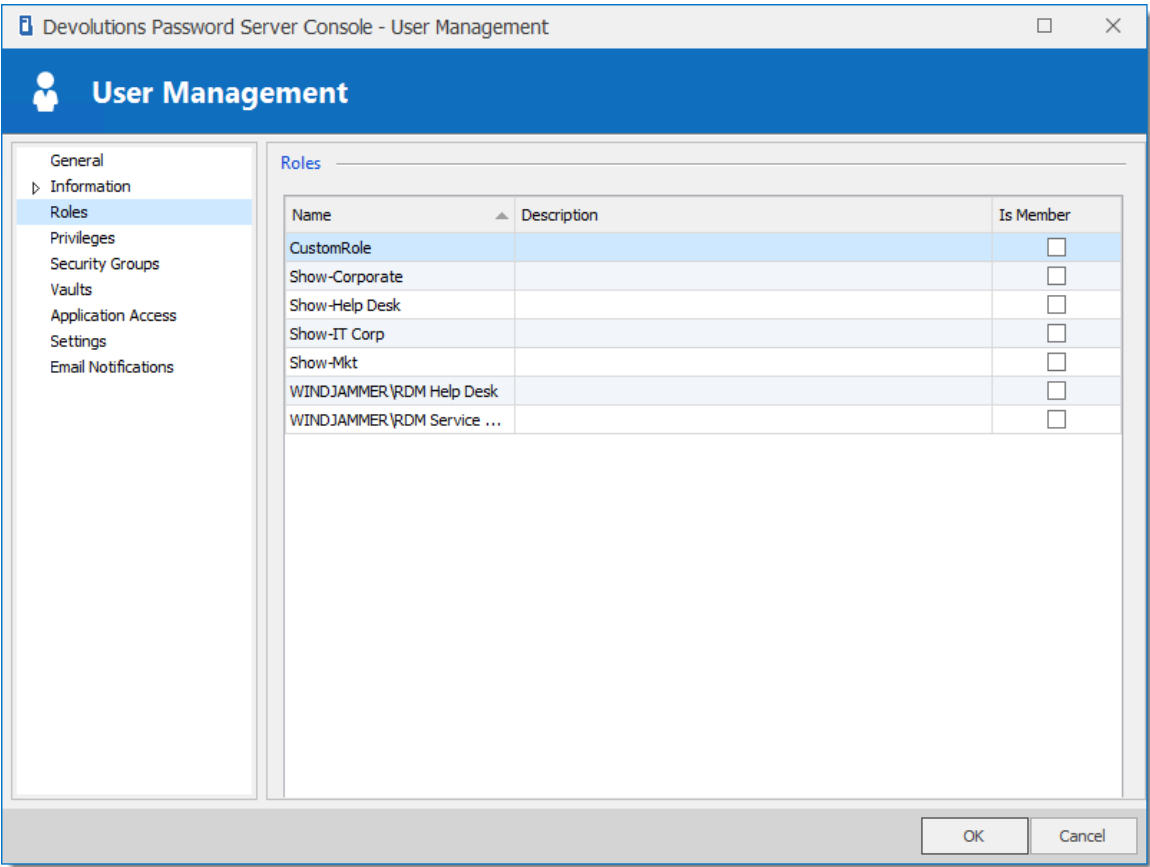
The **Information** section allows for storing information regarding the users, such as their name, address, and more. The Information section is divided in three sub-sections: **Details, Address, Phone**.

The screenshot shows a window titled "Devolutions Password Server Console - User Management". The window has a blue header bar with a user icon and the text "User Management". On the left side, there is a sidebar menu with the following items: General, Information (selected), Roles, Privileges, Security Groups, Vaults, Application Access, Settings, and Email Notifications. The main area of the window is titled "Information" and contains several input fields: Company, Job title, Department, Gravatar email, and Language (a dropdown menu currently showing "English"). At the bottom right of the window, there are "OK" and "Cancel" buttons.

User Management - Information

ROLES

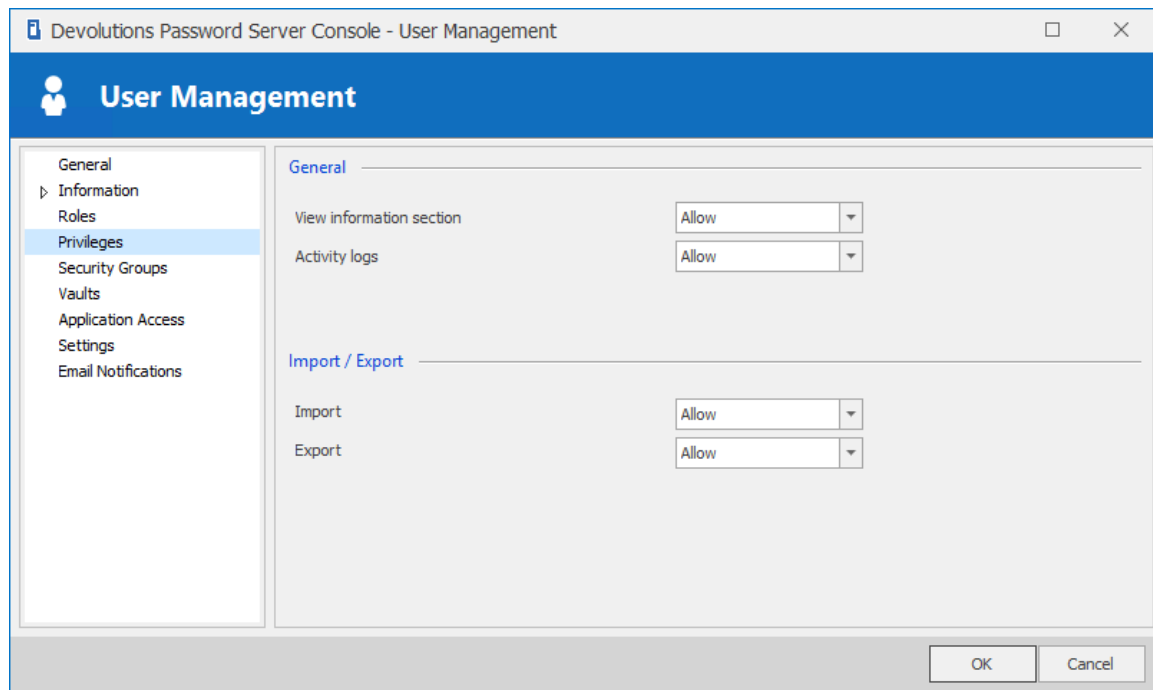
Select roles to assign to the user.



User Management - Roles

OPTION	DESCRIPTION
Roles	Check the Is Member box to assign the role to the user. Consult Role Management topic for more information.

PRIVILEGES



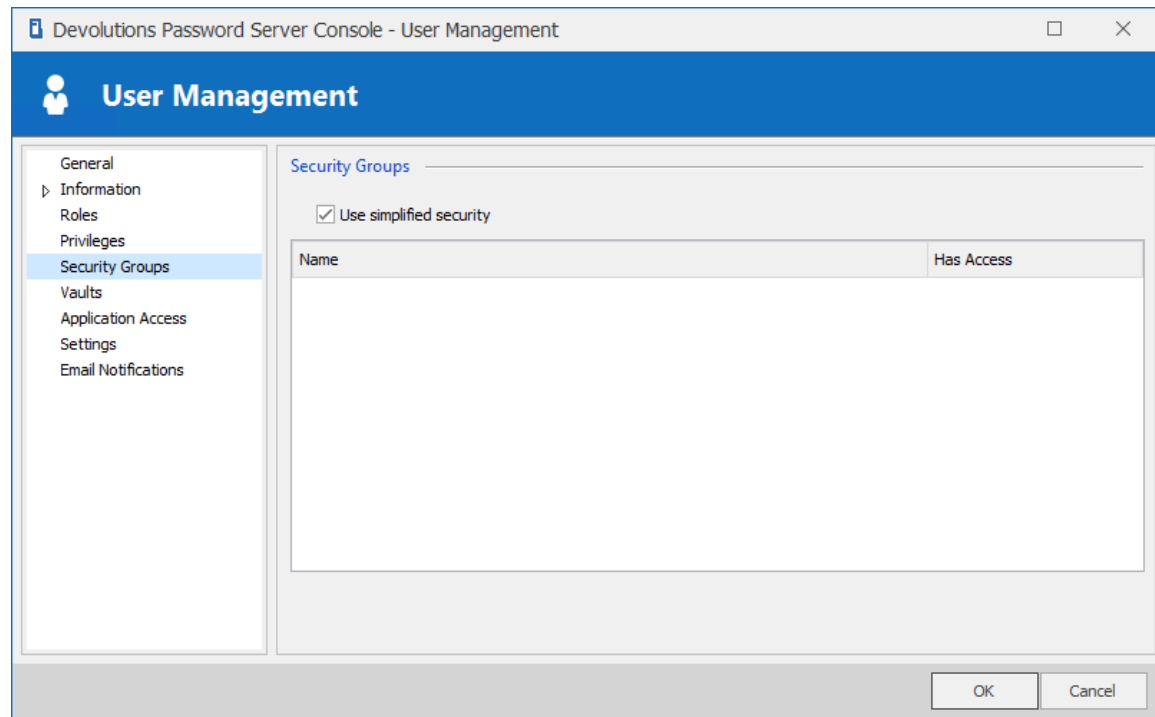
User Management - Privileges

OPTION	DESCRIPTION
View information section	Allows the user to see the content of the Information tab for all sessions.
Activity logs	Allows the user to see the content of the Logs that applies to a session.
Import	<p>Allows the user to Import sessions (Clipboard - Paste as well).</p> <p>The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.</p>
Export	<p>Allows the user to Export sessions (Clipboard - Copy as well).</p> <p>The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.</p>

SECURITY GROUPS (LEGACY)

The **Security Groups** section manages permissions with **Security Groups**.

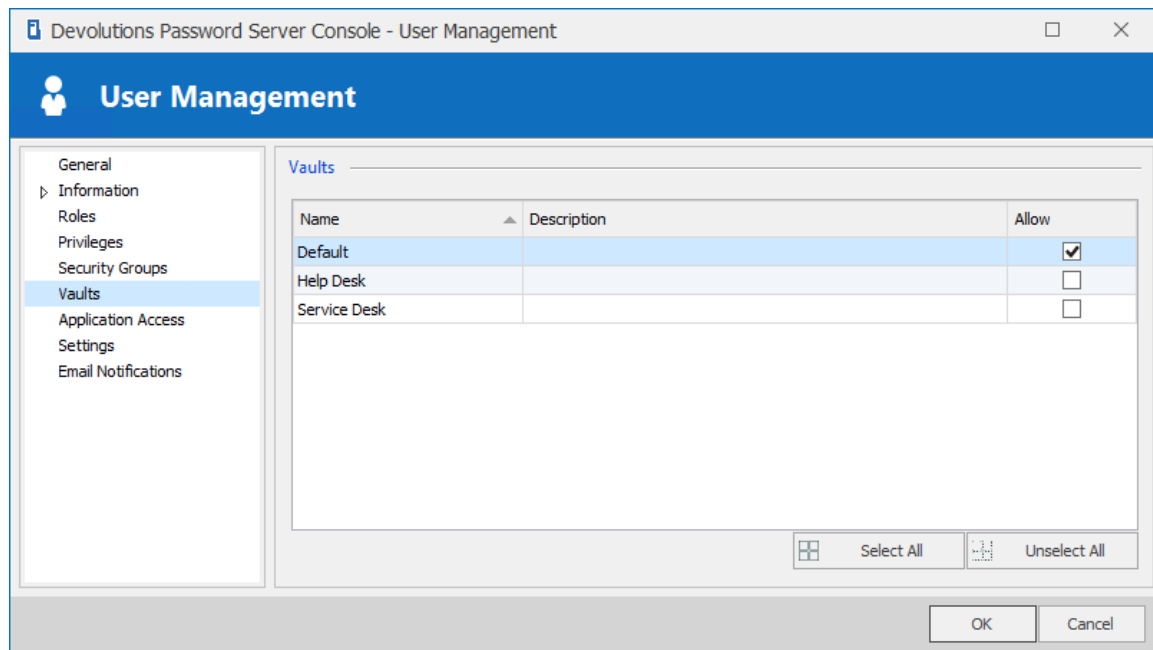
We do not recommend using this method, it is now considered a Legacy setting and is best replaced by the [Role Management](#).



User Management - Security Groups

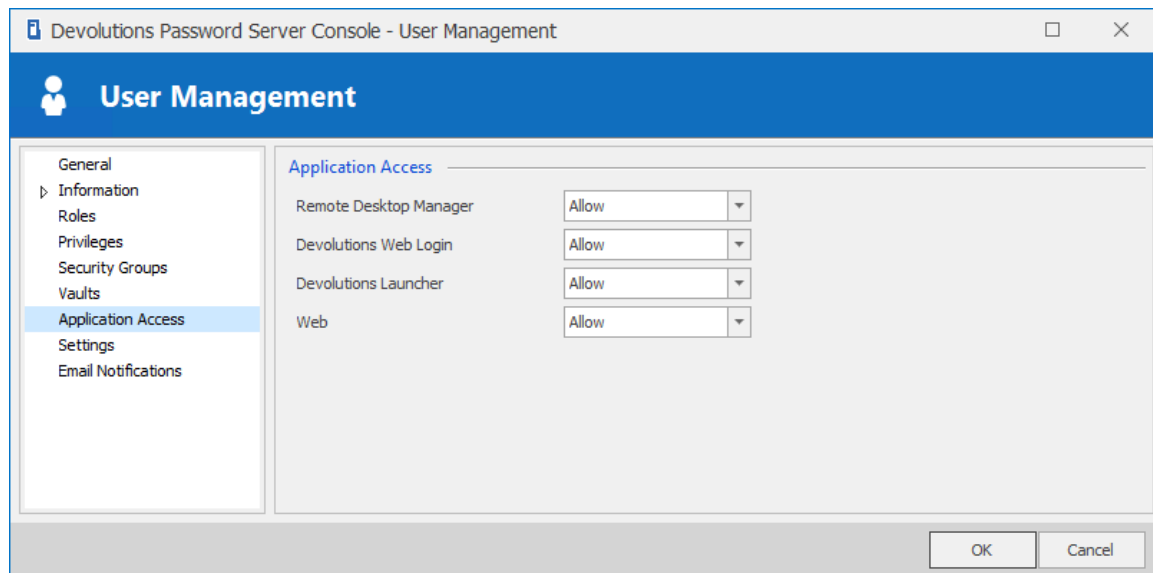
VAULTS

Select which **Vaults** the user has access to.

*User Management - Vaults*

APPLICATION ACCESS

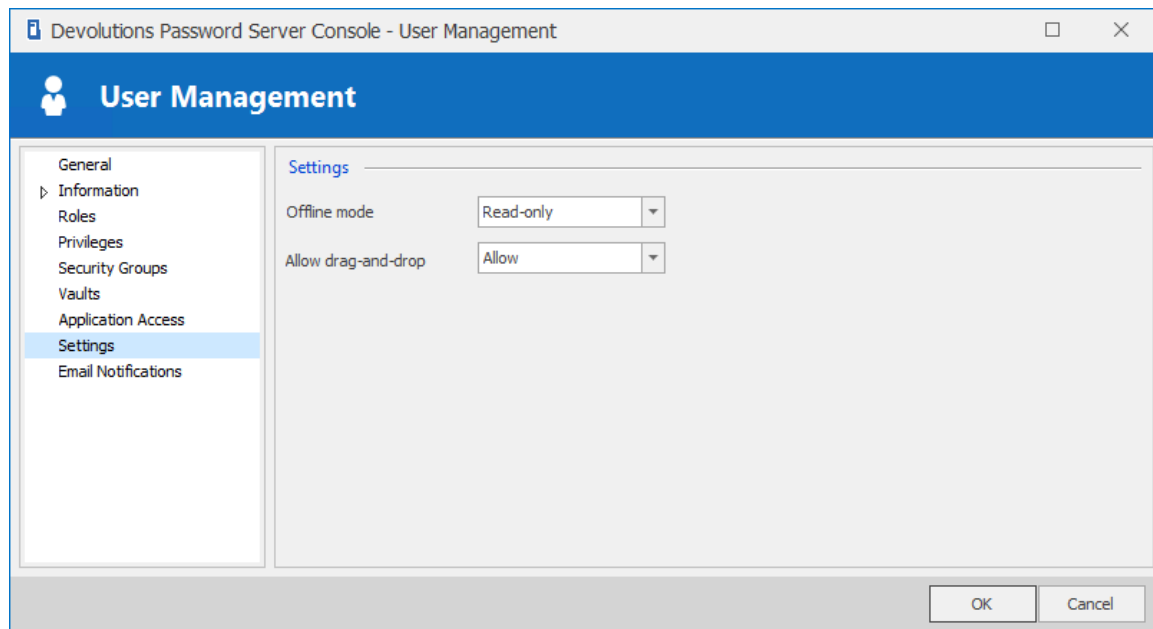
Select which application the user will be allowed to use.

*User Management - Application Access*

OPTION	DESCRIPTION
Remote Desktop Manager	Allows the user to connect to Devolutions Server instance using Remote Desktop Manager application.
Devolutions Web Login	Allows the user to connect to Devolutions Server instance using Devolutions Web Login browser extension.
Devolutions Launcher	Allows the user to connect to Devolutions Server instance using Devolutions Launcher.
Web	Allows the user to connect to the Web Interface of Devolutions Server.

SETTINGS

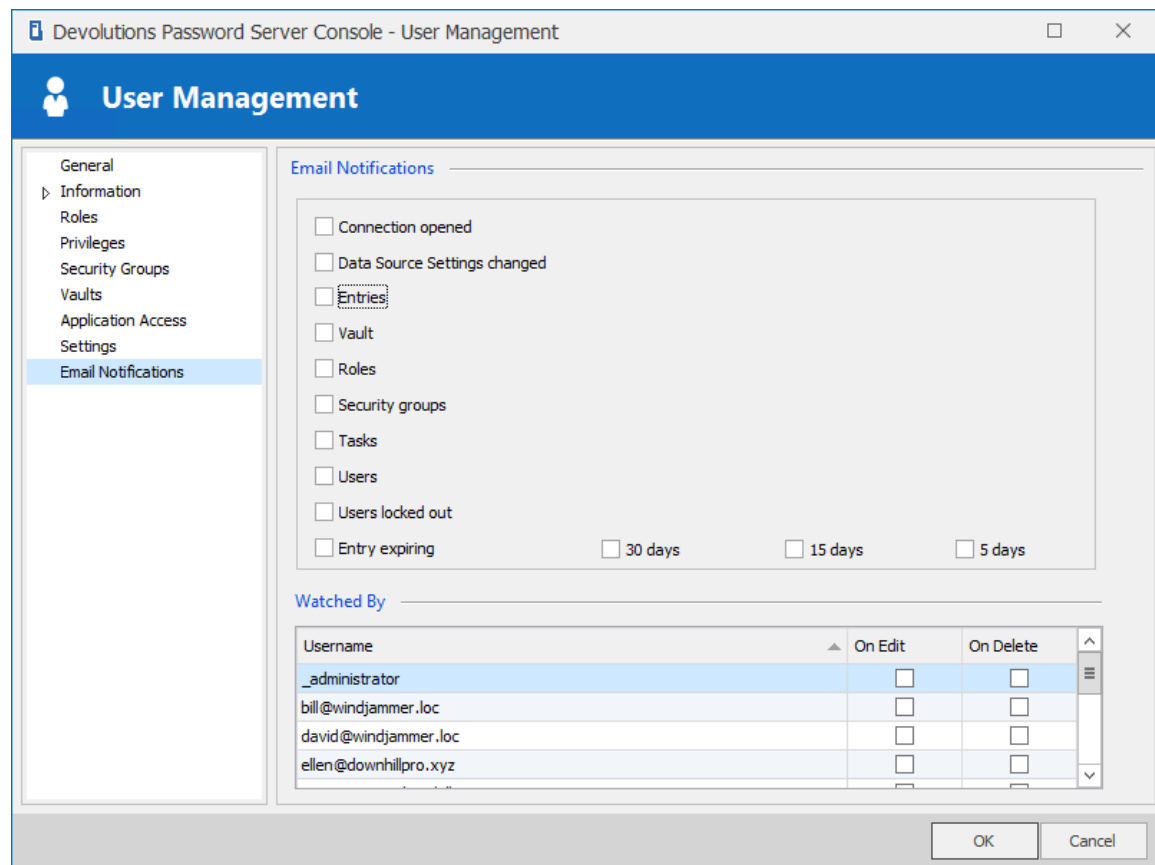
Allow the user to enable the [Offline Mode](#) and whether or not they can use the Drag-n-Drop feature.



User Management - Settings

EMAIL NOTIFICATIONS

Email Notifications are used to send email notifications to specific users. These notifications include any activities on sessions, security groups, roles, users, etc. The notifications will be sent whenever the selected event occurs.



User Management - Email Notifications

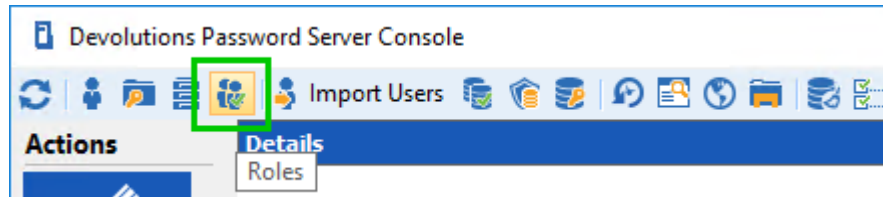
4.3.2 Role Management

DESCRIPTION

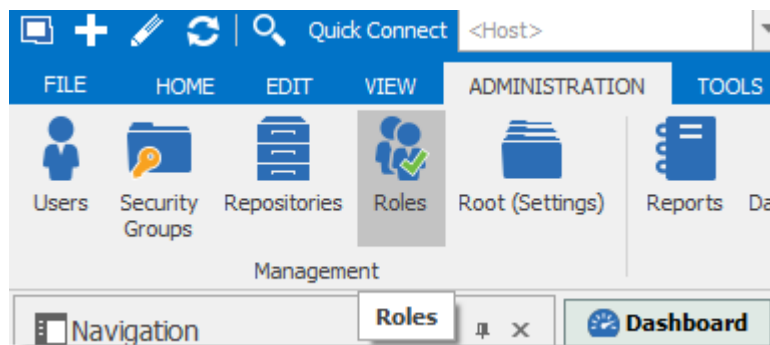


Active Directory groups must be created before creating Roles.

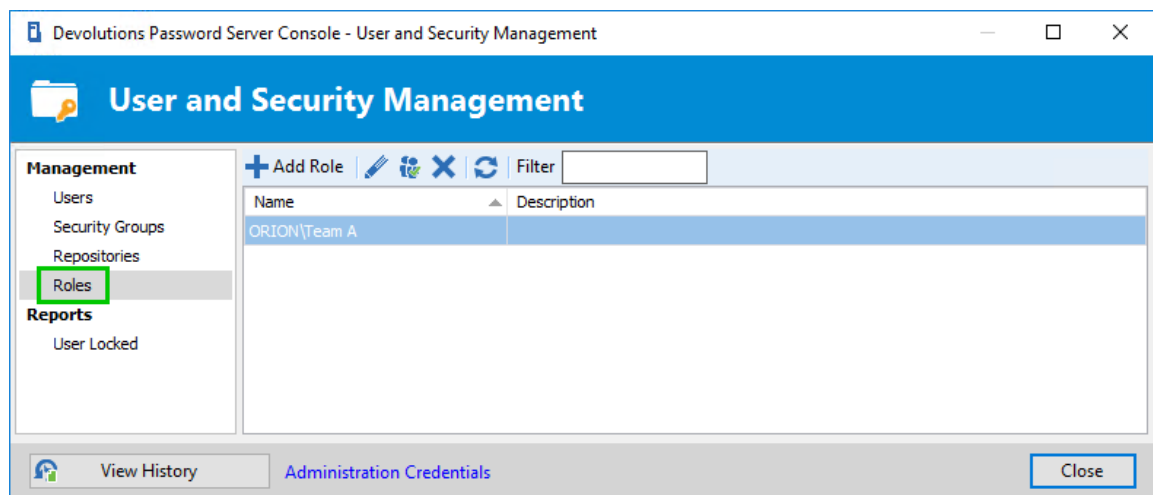
Roles in Devolutions Server are mainly used to reduce the time taken to manage users. The management of permissions granted to roles are quite similar to the corresponding notions for users, but instead of a single user, they apply to all users to which you've assigned the role. This allows the server to link an Active Directory (AD) group to a role in Devolutions Server. Once a domain user logs in the Devolutions Server data source, their user account will be created if needed and users rights will be controlled by the defined groups.



Manage Roles in Devolutions Password Server Console



Manage Roles in Remote Desktop Manager

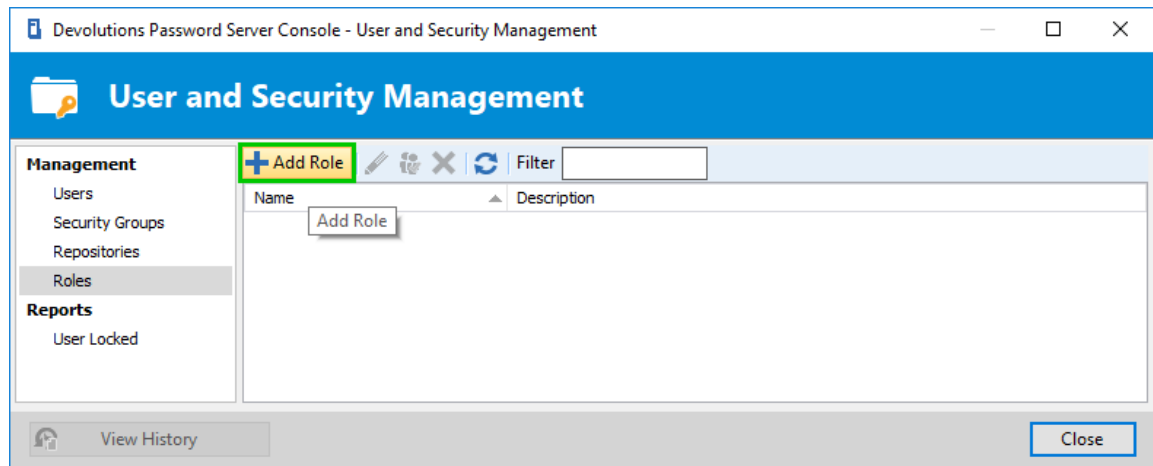


Roles Management Dialog

SETTINGS

CREATE ROLES

To create a new role in your data source click on **Add Role**.



Role Management - Add Role

ROLE MANAGEMENT SETTINGS

GENERAL

Devolutions Password Server Console - Role Management

Role Management

General

Privileges

Security Groups

Vaults

Users

Email Notifications

General

ID: 5C565F4D-B155-4306-8EAC-2C82678EEFD7

Name: ...

Description:

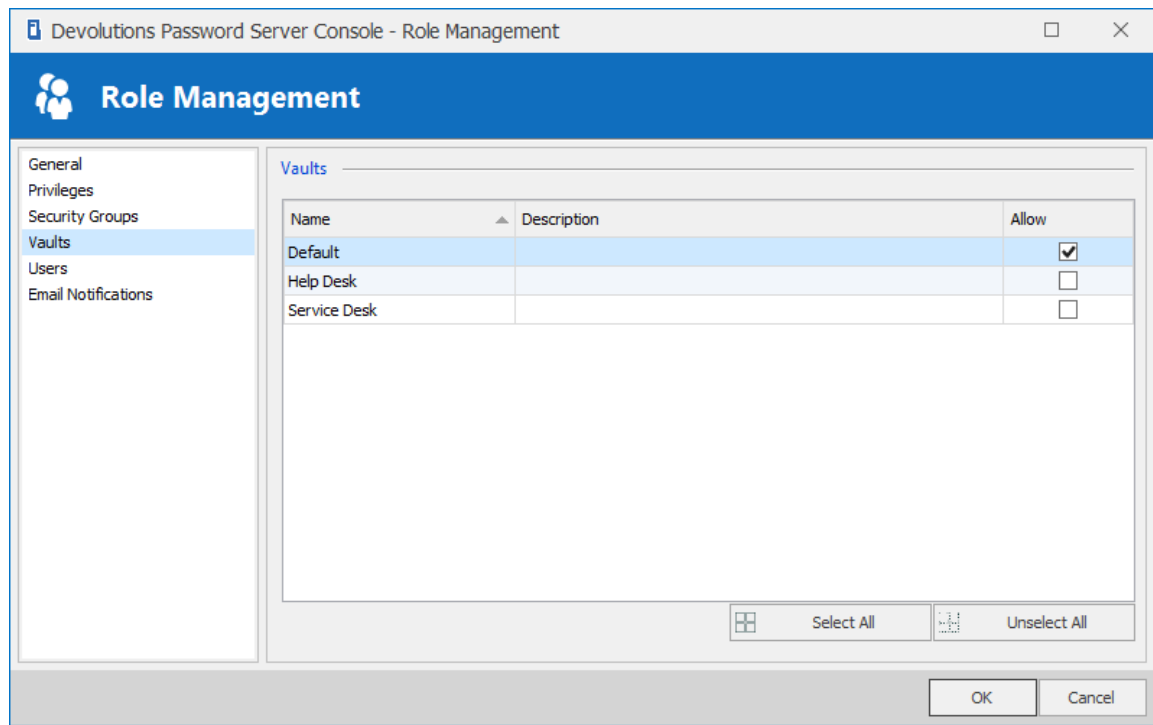
☐ Administrator

OK Cancel

Role Management - General

OPTION	DESCRIPTION
Name	Enter a name for your new Role. The ellipsis button on the right allows to browse the Active Directory structure to select an Active Directory Group as the name of the new Role.
Description	Enter a short description of your new Role.
Administrator	If enabled, the Role is set with Administrator privileges and all users bind to this role will inherit Administrator privileges in Devolutions Server.

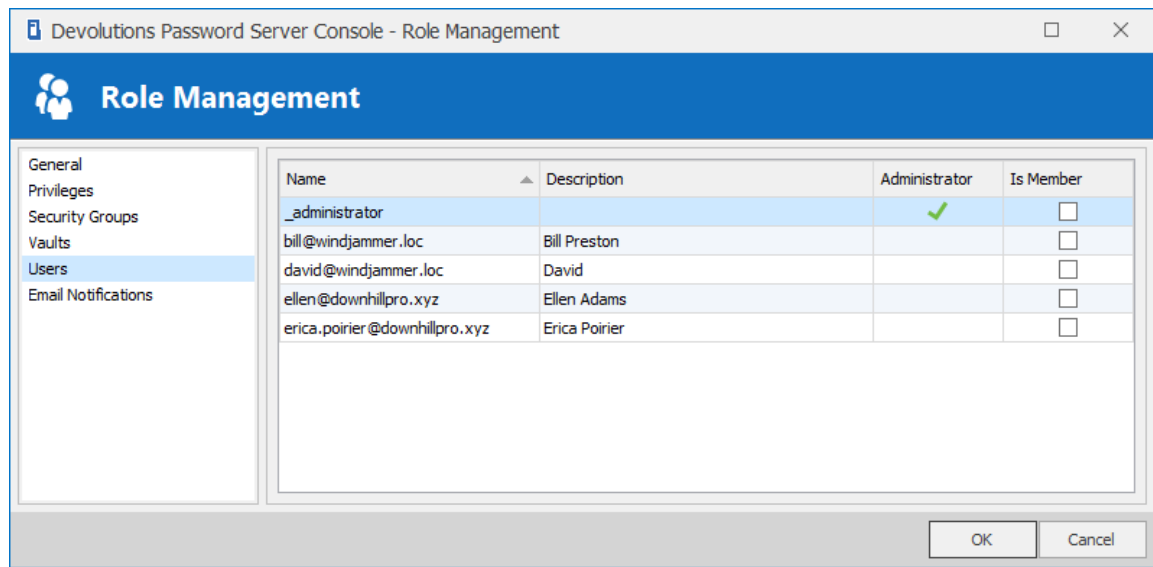
VAULTS

*Role Management - Vaults*

OPTION	DESCRIPTION
Vaults	Consult the Vaults topic for more information.

USERS

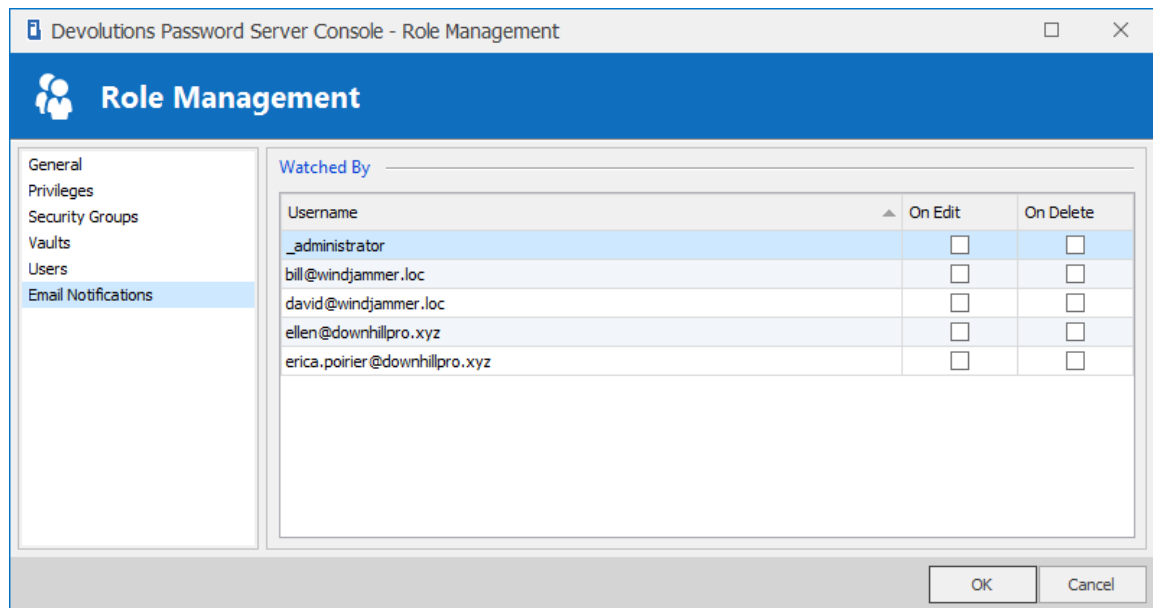
Here you can assign users the current role. You can also reassign them later on.



Role Management - Settings

EMAIL NOTIFICATIONS

Email Notifications are used to send email notifications to specific users.



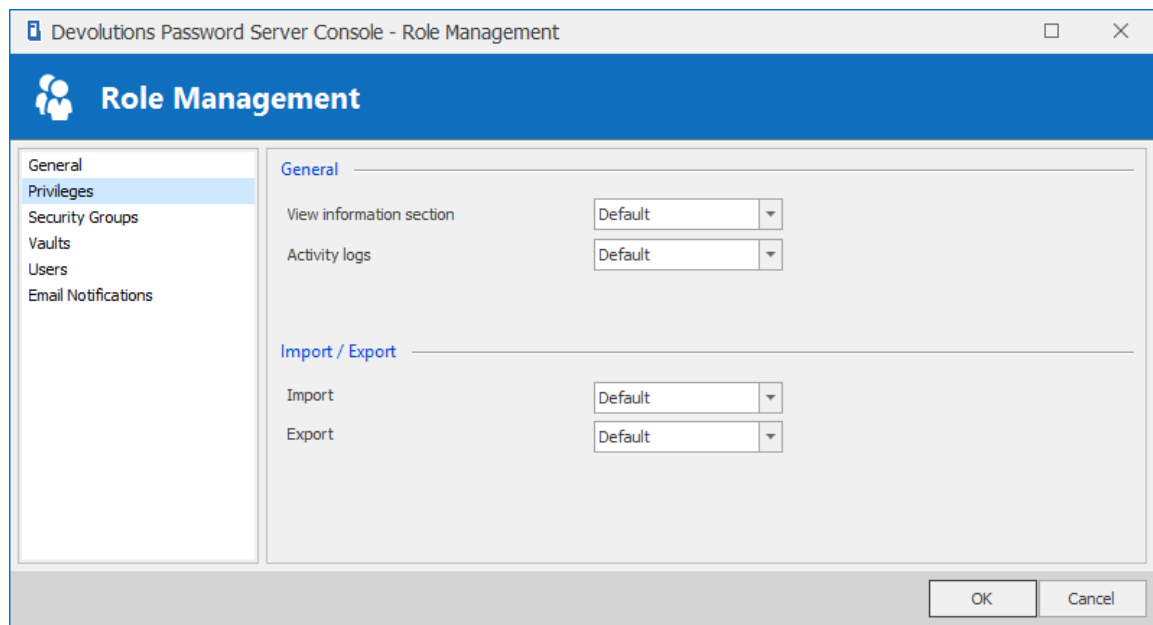
Role Management - Email Notifications

OPTION	DESCRIPTION
Username	If enabled, will send notification to the user about modifications on this role. It could be set on specific operation (Edit and/or Delete).

4.3.2.1 Legacy properties

DESCRIPTION

PRIVILEGES

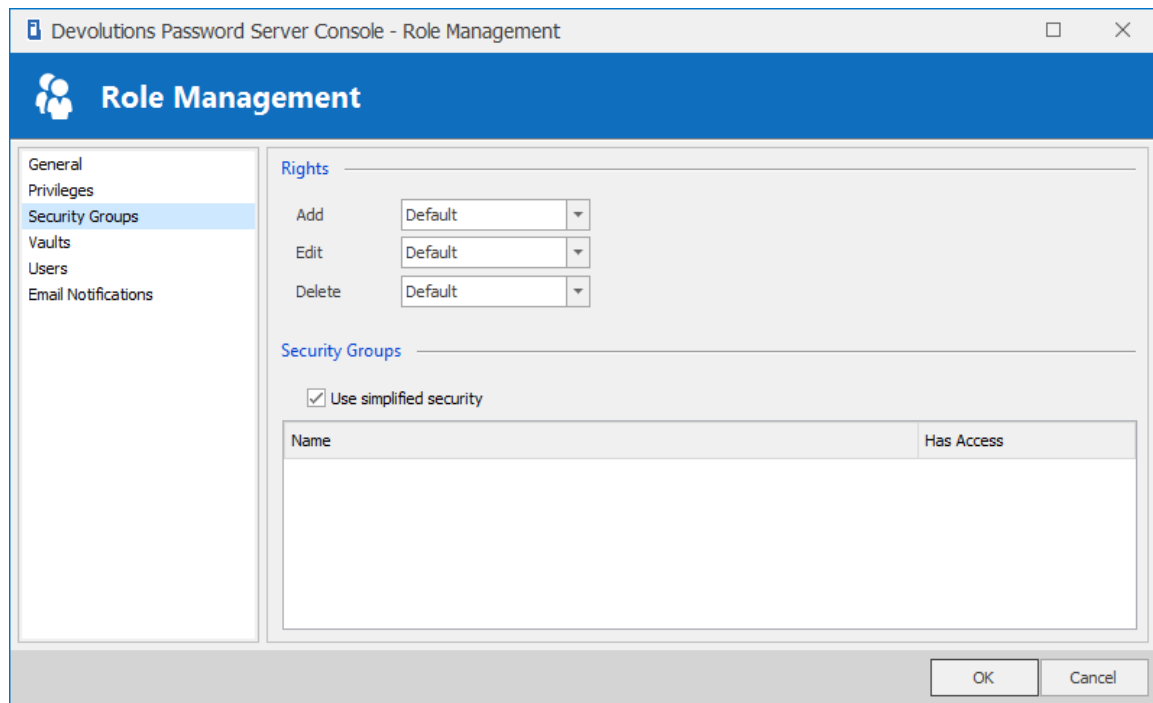


Role Management - Privileges

OPTION	DESCRIPTION
View information section	Allows the user to see the content of the Information tab for all sessions.

OPTION	DESCRIPTION
View shared logs	Allows the user to see the content of the Logs that applies to a session.
Import	<p>Allows the user to Import sessions (Clipboard - Paste as well).</p> <p>The import menu (File - Import) and the import feature in the context menu will be grayed out if the option is not active.</p>
Export	<p>Allows the user to Export sessions (Clipboard - Copy as well).</p> <p>The export menu (File - Export) and the export feature in the context menu will be grayed out if the option is not active.</p>

SECURITY GROUPS



OPTION	DESCRIPTION
Rights	Allows Add, Edit and/or Delete rights or blocks Add in root right.
Security Groups	To learn more about Permissions please see the System Permissions topic.

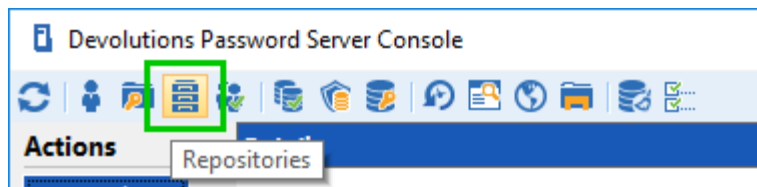
4.3.3 Vault Management

DESCRIPTION

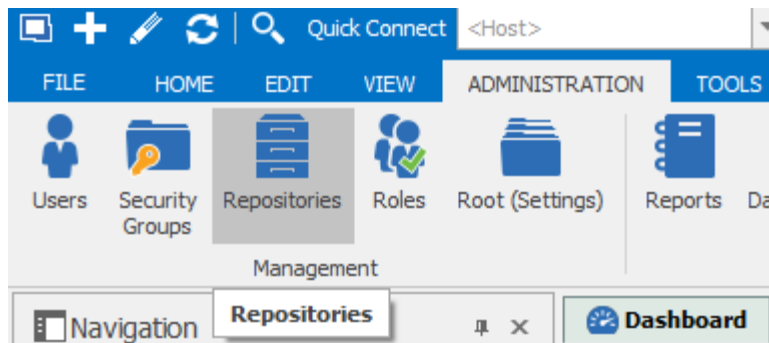
Vaults divide a database in multiple, smaller compartments. Instead of handling the whole database as a single block of data, each **Vault** handles its own subset of entries. As a result, you can manage a massive amount of entries without experiencing reduced performance. All **Vaults** common to a database have the same set of users and roles. Only entries differ from one **Vault** to another.



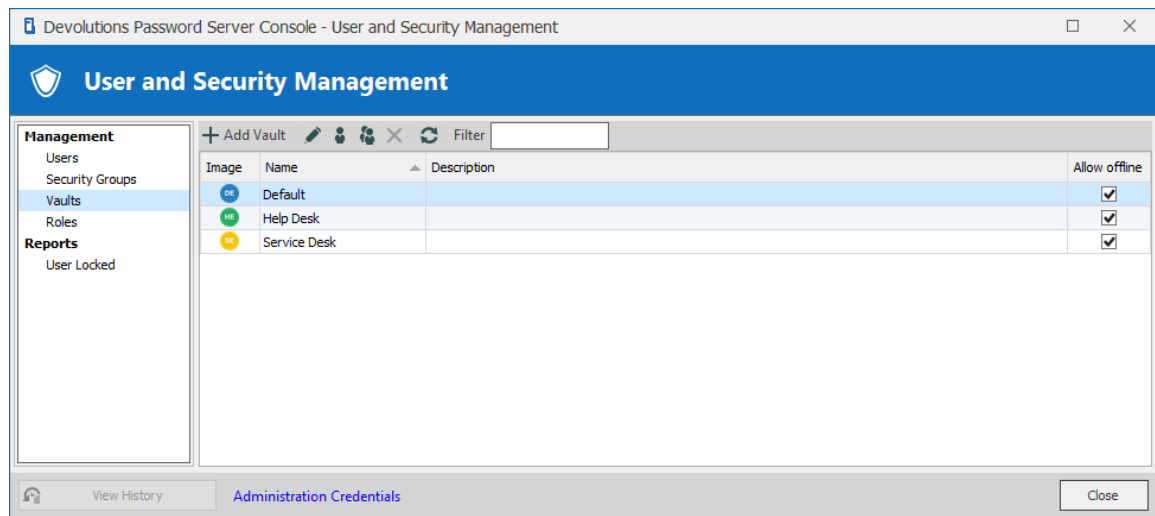
If you have more than 3500 entries stored in your data source and start experiencing performance issues, we strongly recommend to use Vaults to split your entries.



Manage Vaults



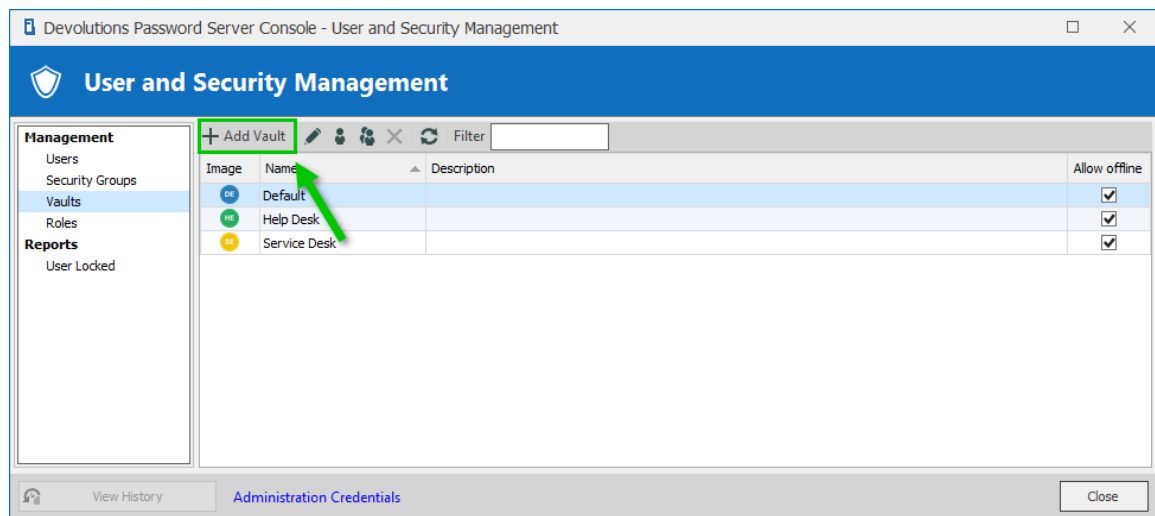
Manage Vaults in Remote Desktop Manager

*Vaults Management Dialog*

SETTINGS

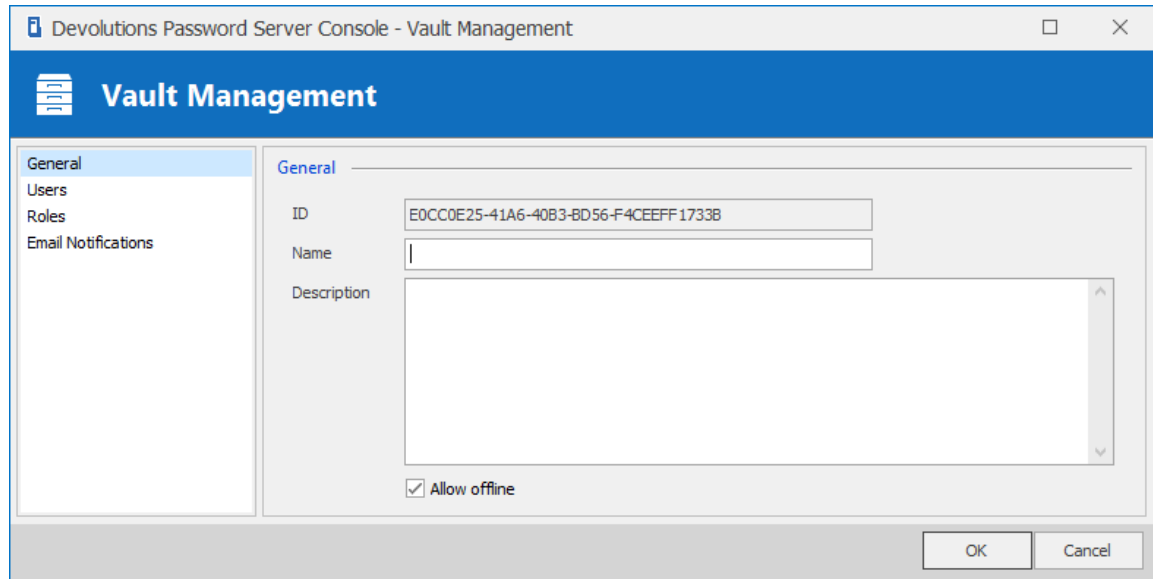
CREATE VAULTS

To create a new Vault in your data source click on **Add Vault**.

*Vaults Management - Add Vault*

VAULT MANAGEMENT SETTINGS

GENERAL

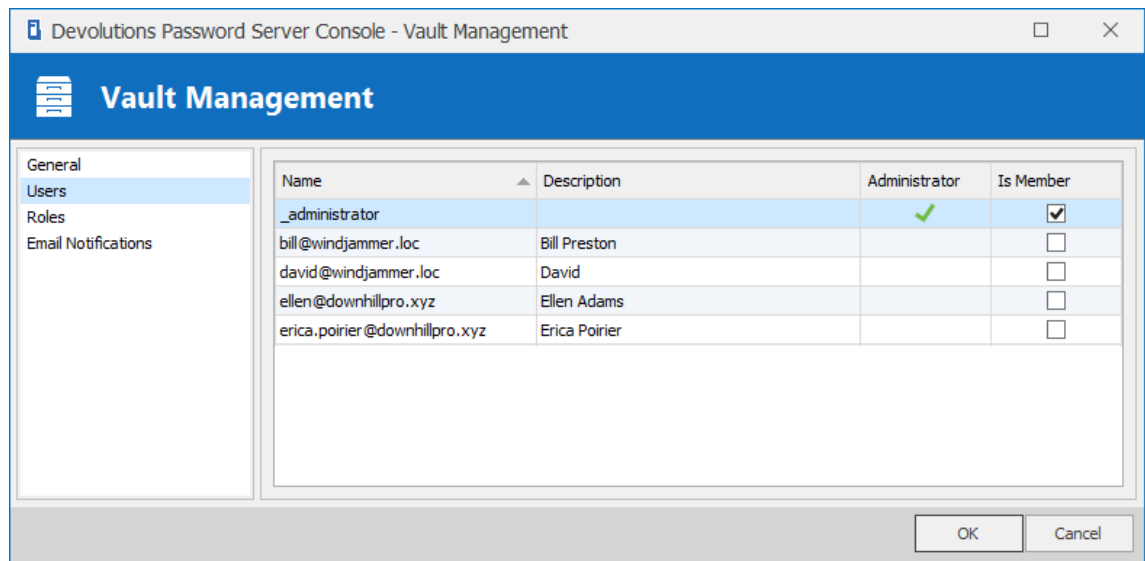


Vault Management - General

OPTION	DESCRIPTION
Name	Enter a name for your new Vault .
Description	Enter a short description of your new Vault .
Allow Offline	Set if the Vault can be used in Offline Mode .

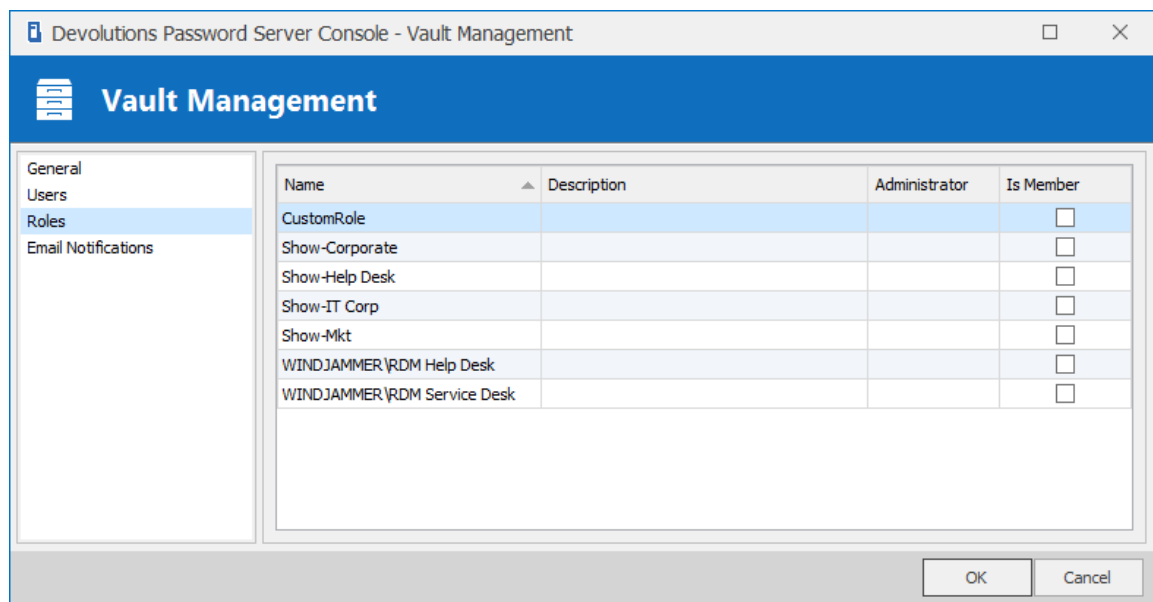
USERS

Select which users should have access to the specific **Vault**. These can be reassigned later.

*Vault Management - Users*

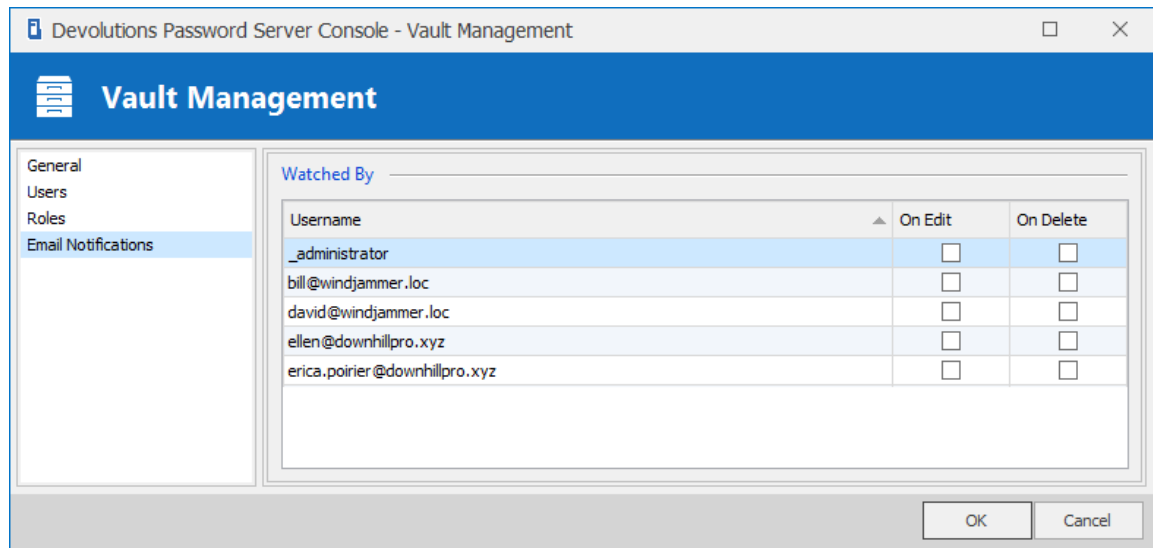
ROLES

Select which roles should have access to the specific **Vault**. All users whom have been assigned these roles will have access to the **Vault**. These can be reassigned later.

*Vault Management - Roles*

EMAIL NOTIFICATIONS

Email Notifications are used to send email notifications to specific users.

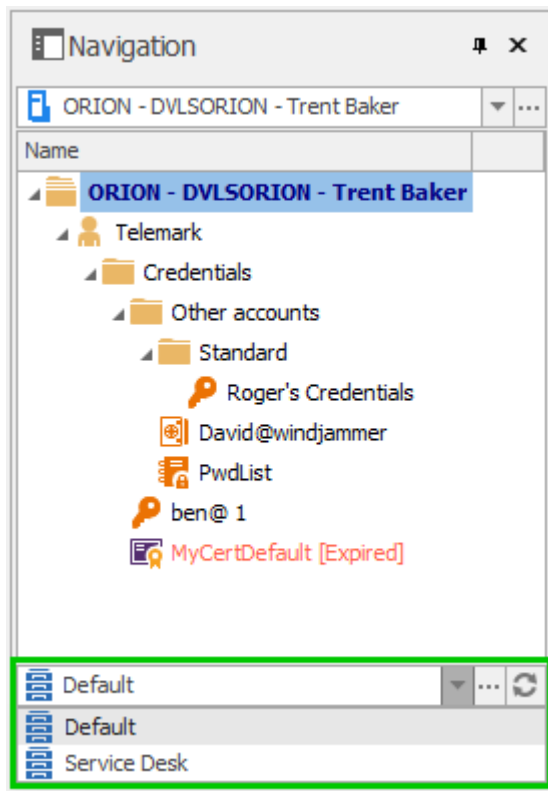


Vault Management - Email Notifications

OPTION	DESCRIPTION
Username	If enabled, will send notification to the user about modifications on this Vault . It could be set on specific operation (Edit and/or Delete).

CONNECT TO A VAULT

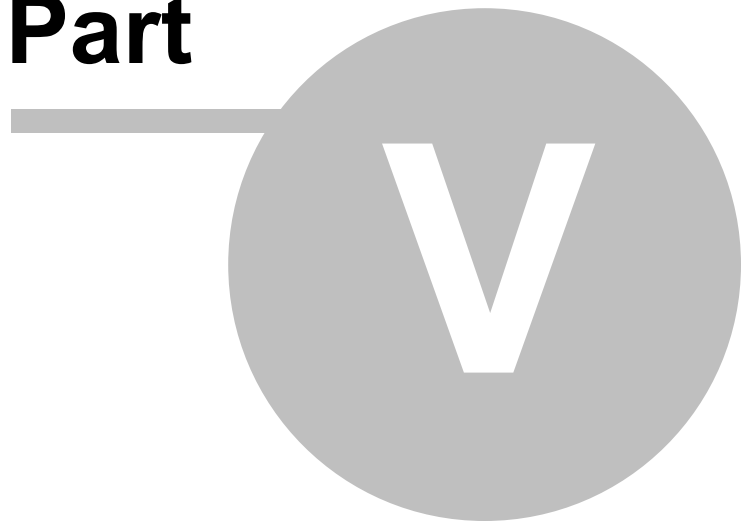
1. Select the data source that connects to the Devolutions Server instance in which the **Vault** has been created.
2. From the **Navigation Pane**, select the desired **Vault**.



Navigation Pane - Vault Selector

Web Interface

Part



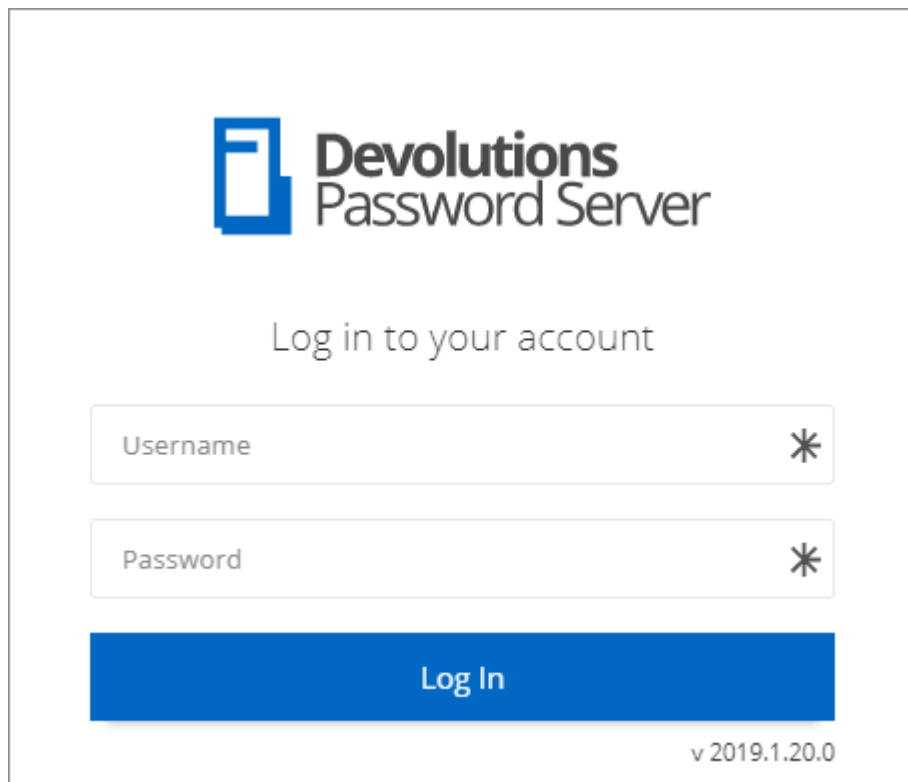
5 Web Interface

DESCRIPTION

The Devolutions Server web interface offers a simplified interface for end-users to use and manage passwords from any web browser.

LOGIN PAGE

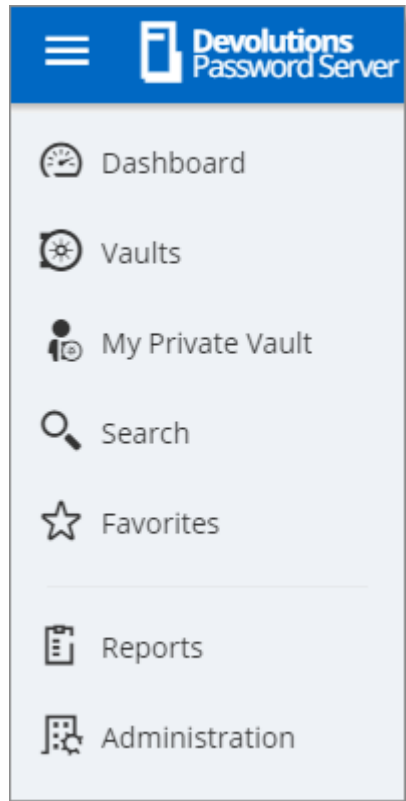
Open a web browser and navigate to the URL of the Devolutions Server instance. If the instance has been created with the default URL, it would be available at `http://<ServerName>/dps`. Simply enter the username and password of a Devolutions Server account to connect.

The image shows a web browser window displaying the login page for Devolutions Password Server. At the top, there is a logo consisting of a blue square with a white stylized 'D' inside, followed by the text 'Devolutions Password Server' in a dark grey sans-serif font. Below the logo, the text 'Log in to your account' is centered. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small asterisk icon to their right. Below the input fields is a large blue button with the text 'Log In' in white. In the bottom right corner of the page, the version number 'v 2019.1.20.0' is displayed.

Devolutions Password Server - Login Page

MENU

The **Menu** allows the user to navigate through the different sections. It can be expanded or collapsed to hide the labels by clicking on the Devolutions Password Server icon the the top-left corner.

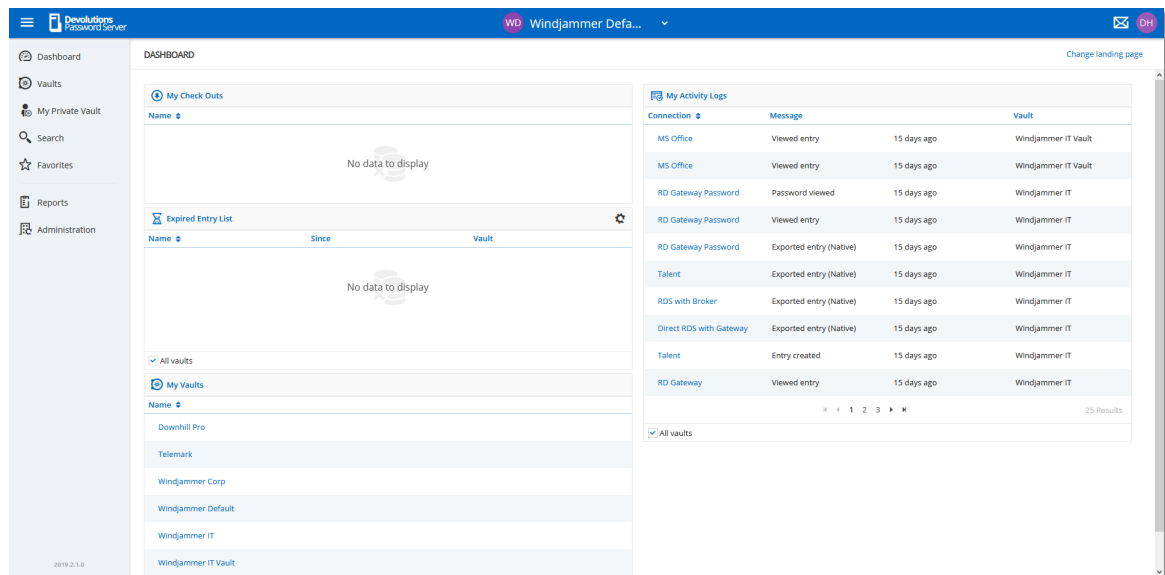


Menu

5.1 Dashboard

DESCRIPTION

The **Dashboard** section provides an overview of the available **My Check Outs**, **Expired Entry List**, **My Vaults** and **My Activity Logs**.



Dashboard

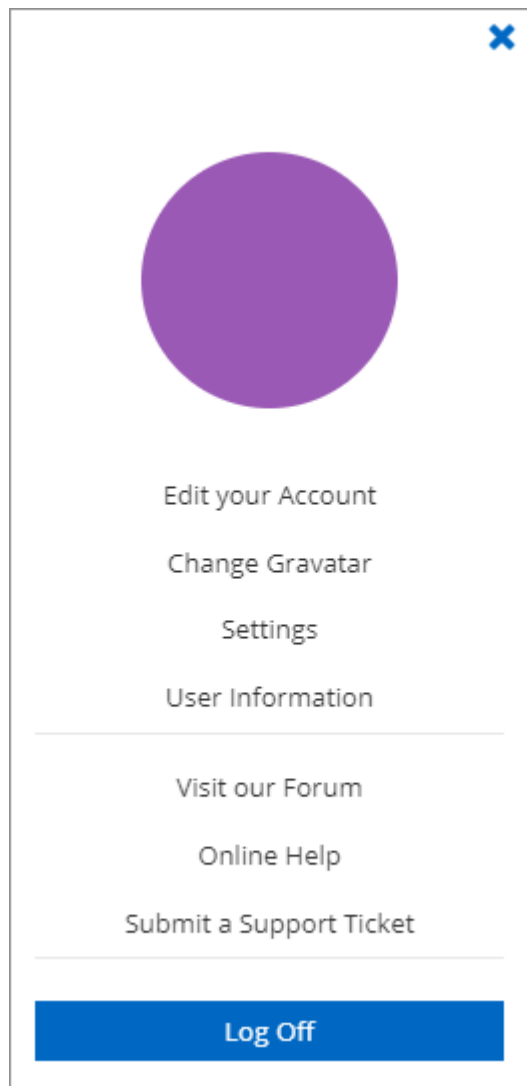
5.2 Account Menu

DESCRIPTION

Users manage their account: language preferences, personal information, Gravatar, as well as limited configuration of the web interface. The menu includes links to Devolutions Online Help and forum. Users log out of Devolutions Server from the **Account Menu**.

SETTINGS

Click the Gravatar or initials to access the **Account Menu**.



Account Menu

EDIT YOUR ACCOUNT

Set the language of the web interface.

Add or modify personal information.

Edit your Account

INFORMATION

GENERAL

First name

Last name

Email

Company

Language

ADDRESS

Address

State

Country

Phone

Work

Mobile

Fax

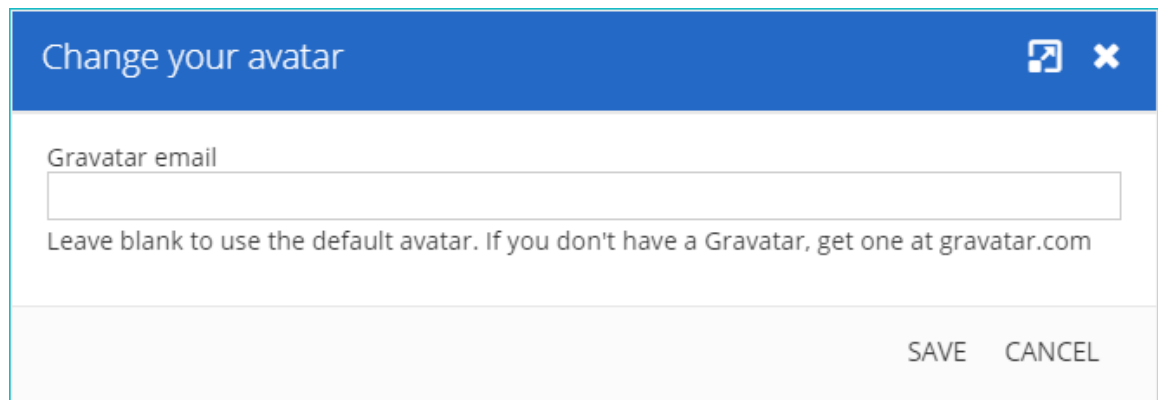
SAVE CANCEL

Edit your Account

CHANGE GRAVATAR

The default user avatar is the user initials. Users can use an image uploaded at Gravatar.com.

Enter the email associated with your Gravatar account.

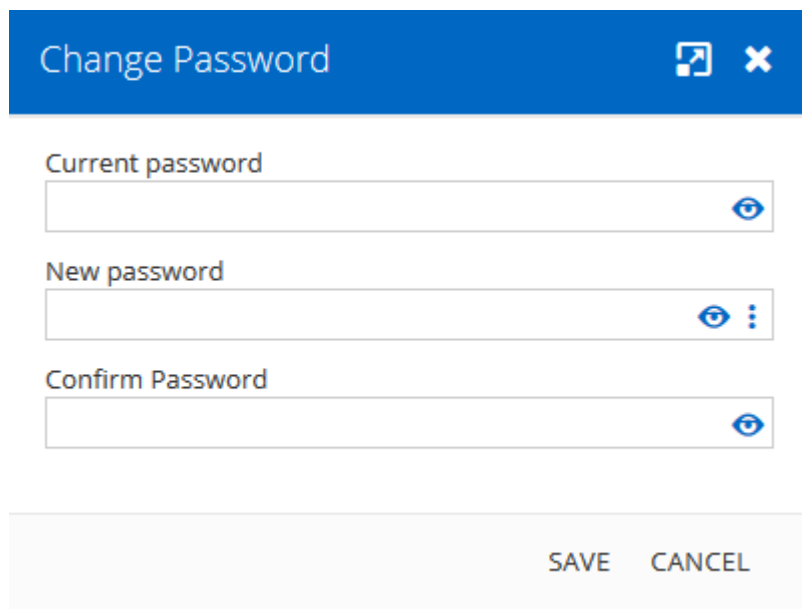


A dialog box titled "Change your avatar" with a blue header bar containing a maximize icon and a close icon. The main area has a label "Gravatar email" above a text input field. Below the field is a hint text: "Leave blank to use the default avatar. If you don't have a Gravatar, get one at gravatar.com". At the bottom right are "SAVE" and "CANCEL" buttons.

Change your Avatar

CHANGE PASSWORD

Allow the user to modify his password. Only available for Devolutions Server Custom or Database account type. Please see [Authentication](#) for more information.

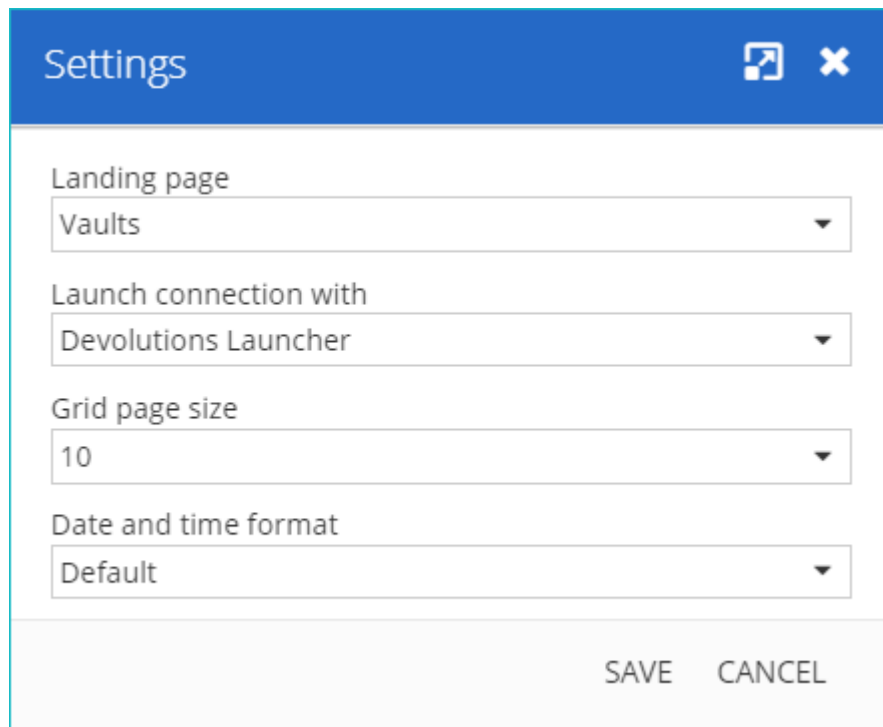


A dialog box titled "Change Password" with a blue header bar containing a maximize icon and a close icon. The main area has three labels: "Current password", "New password", and "Confirm Password", each followed by a password input field. Each field has a toggle icon (an eye) to the right. The "New password" field also has a three-dot menu icon. At the bottom right are "SAVE" and "CANCEL" buttons.

Change Password

SETTINGS

Modify **User Interface** elements.



Settings

Landing page
Vaults

Launch connection with
Devolutions Launcher

Grid page size
10

Date and time format
Default

SAVE CANCEL

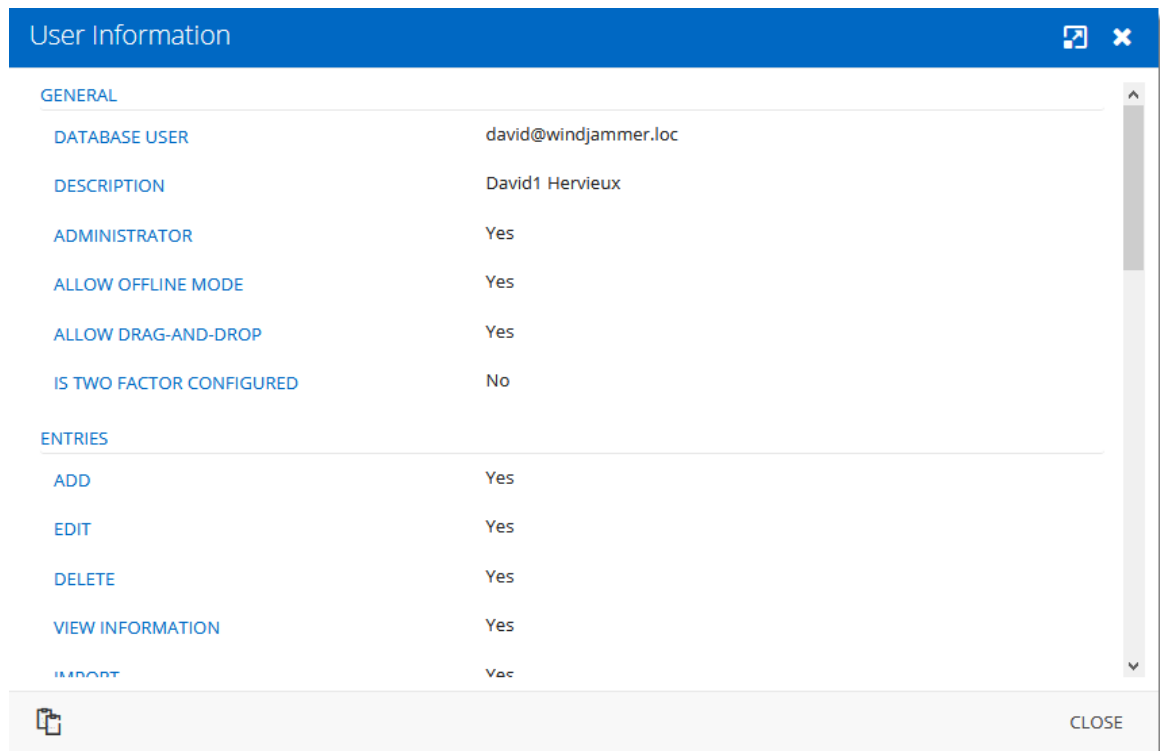
User Interface Settings

OPTION	DESCRIPTION
Landing page	Choose the home page that opens when you sign on: <ul style="list-style-type: none">• Dashboard• Vaults• My Private Vault• Reports• Administration
Launch connection with	Choose the application that opens remote connections: <ul style="list-style-type: none">• Default: refers to Devolutions Launcher• Remote Desktop Manager• Devolutions Launcher

OPTION	DESCRIPTION
Grid page size	Choose the number of rows displayed in lists (e.g. reports) <ul style="list-style-type: none">• 10• 20• 30
Date and time	Choose a format: <ul style="list-style-type: none">• Default: month/day/year• US• Custom

USER INFORMATION

Display the User Information report that contains the user account configuration.



GENERAL	
DATABASE USER	david@windjammer.loc
DESCRIPTION	David1 Hervieux
ADMINISTRATOR	Yes
ALLOW OFFLINE MODE	Yes
ALLOW DRAG-AND-DROP	Yes
IS TWO FACTOR CONFIGURED	No

ENTRIES	
ADD	Yes
EDIT	Yes
DELETE	Yes
VIEW INFORMATION	Yes
IMPORT	No

VISIT OUR FORUM

A link to our forum for support and feature requests.

ONLINE HELP

A link to our online user guides.

SUBMIT A SUPPORT TICKET

Submit the **Data Source Information** and **Diagnostic Report** to the Devolutions Support team.

Send Report to Support ✕

PERSONAL INFORMATION

Email

Company

Name


☒ Send data source information


☒ Diagnostic information

MESSAGE

Subject

Detail

 SEND TO SUPPORT ▼ CANCEL

 Download the Zip

OPTION	DESCRIPTION
Email	Provide your email address.
Company	Provide your company name.
Name	Provide your name.

OPTION	DESCRIPTION
Send data source information	When enabled, the Data Source Information report will be attached to the email.
Diagnostic information	When enabled, the Diagnostic report will be attached to the email.
Subject	Subject of the message.
Detail	Additional information or detail can be enter in the Detail section.
Send to Support	Will send this Report to Devolutions Support team.
Download the Zip	Allows to download the Report into a Zip file that can be saved on your local computer.
Cancel	Cancel the operation.

LOG OFF

Sign off from your account.

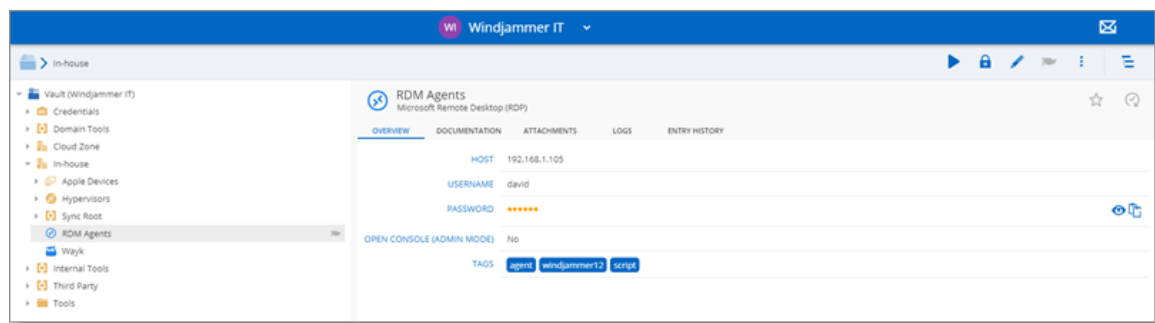
5.3 Vaults

DESCRIPTION

The **Vaults** allows the users to [create entries](#) and manage the content of the data source. Vaults are divided in two parts:

- The **Navigation Pane** (left) lists the entries available in the data source (current Vault).

- The **Content Area** (right) displays information regarding the selected entry.

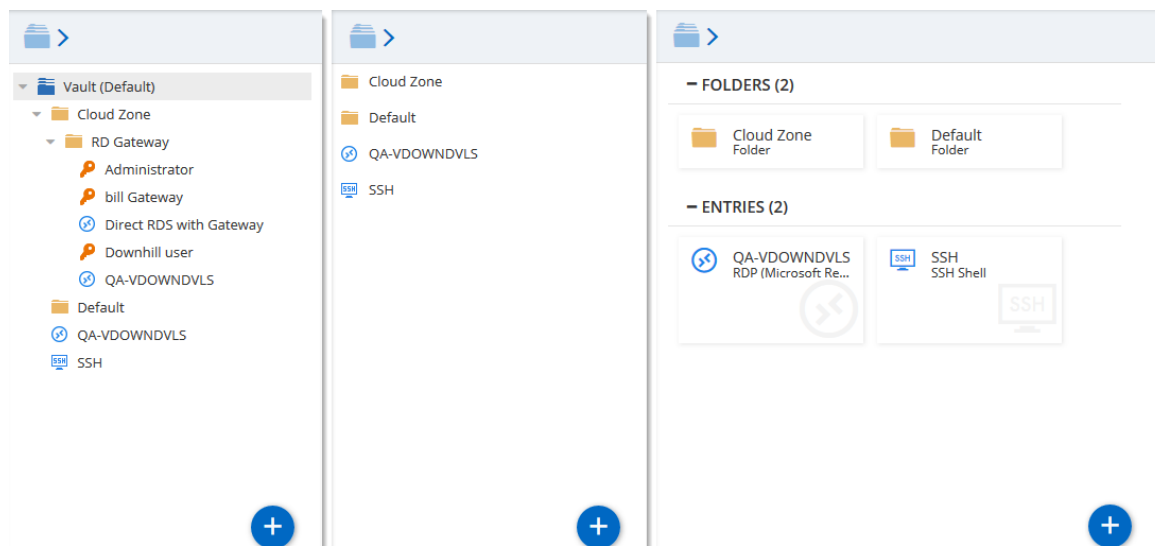


Vaults

NAVIGATION PANE

The **Navigation Pane** displays the entries available to the user. The **Navigation Pane** can display entries in three different manners:

- **Tree View**
- **List View**
- **Grid View**



Navigation Pane - Tree View (left), List View (center) and Grid View (right)

DASHBOARD

The **Content Area** displays various information regarding the selected entry.

The screenshot shows the 'Entry Overview' for a session named 'QA-VDOWNDVLS' (Microsoft Remote Desktop (RDP)). The interface includes a top toolbar with icons for play, check out, view password, edit, status, and more options. Below the session name, there are tabs for OVERVIEW, DOCUMENTATION, ATTACHMENTS, LOGS, and ENTRY HISTORY. The main content area displays the following details:

HOST	QA-VDOWNDVLS.downhill.loc
USERNAME	administrator
DOMAIN	downhill
PASSWORD	•••••
OPEN CONSOLE (ADMIN MODE)	No

Entry Overview

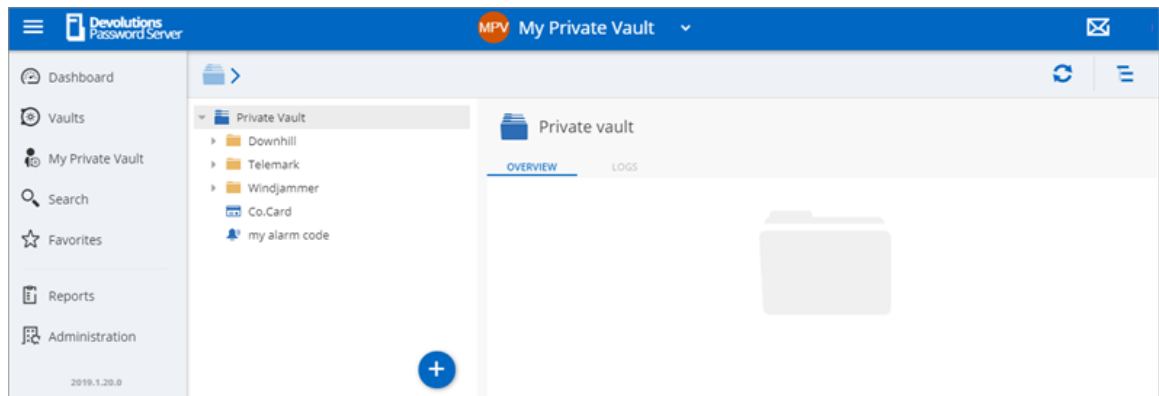
OPTIONS	DESCRIPTION
Open ▶	Open the session (Devolutions Launcher required).
Check Out ⌚	Check Out the session.
View Password 🔒	View the password of the selected entry.
Properties ✎	Edit the properties of the selected entry.
Status 🚩	Edit the status of the selected entry.
More ⋮	Display more options for the selected entry. <ul style="list-style-type: none"> • User Specific Settings • Save as Template • View Password History

OPTIONS	DESCRIPTION
	<ul style="list-style-type: none"> • Delete
Add to Favorites ☆	Add the selected entry to favorites.
Statistics 🔄	Hover the icon to view who has created/modified the entry.
View Password 👁	Display the password of the selected entry.
Copy to clipboard 📄	Copy the field of the selected entry (Usually Username or Password).

5.3.1 My Vault (Private)

DESCRIPTION

The **Private Vault** is a user specific **Vault** used to store private information, credentials and passwords. It allows each user to have their very own private **Vault** that only they can access, not even an administrator could access them. The **Private Vault** prevents users from using a non-secure tool to manage their personal passwords at work.



Private Vault

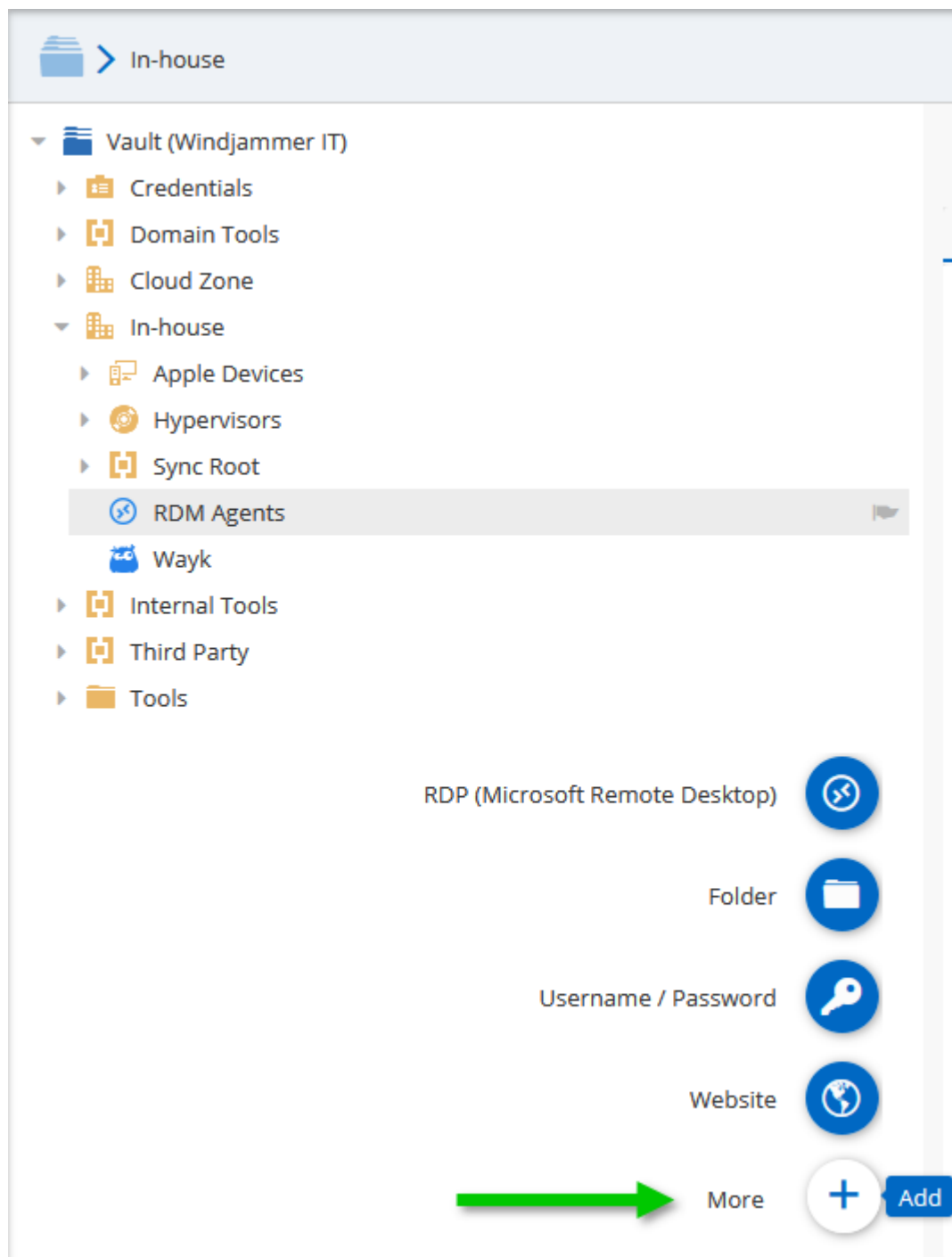
5.3.2 Create a New Entry

DESCRIPTION

Every item you see in your Vault and Private Vault is an **Entry**. There are many type of entries that can be created directly in Devolutions Server web interface.

CREATING A NEW ENTRY

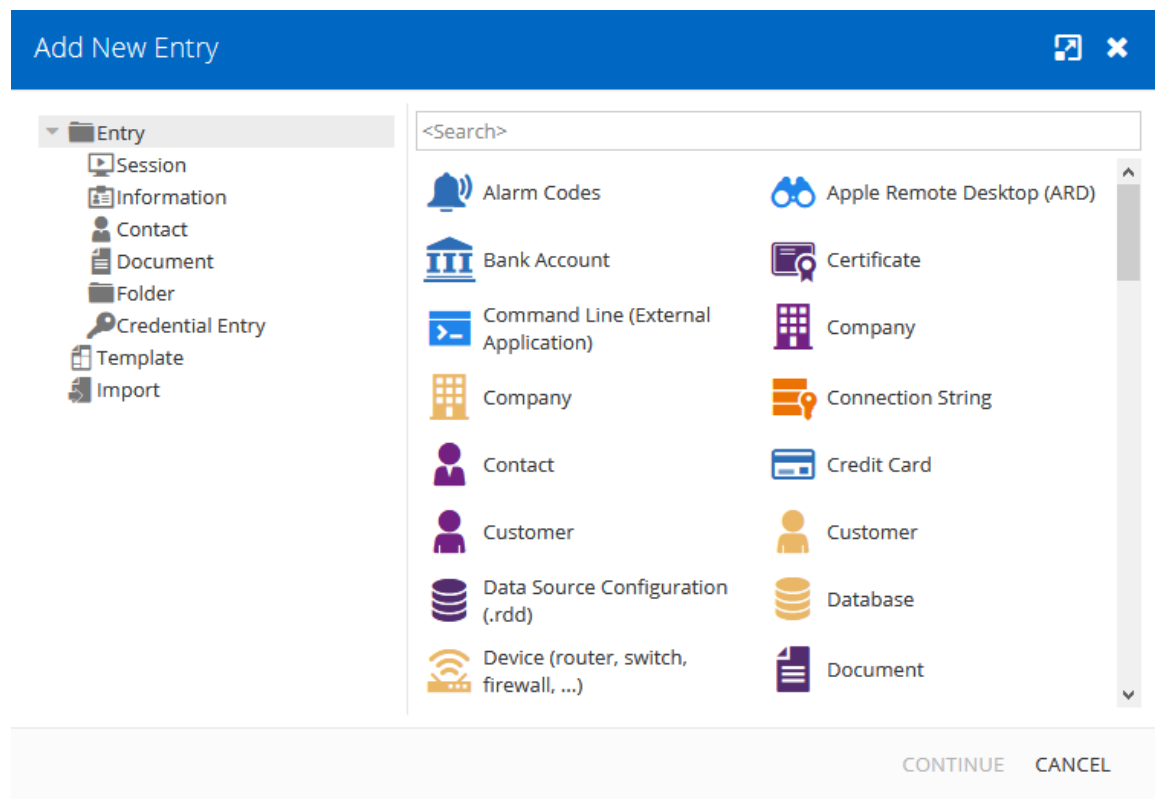
To create a new entry go in the Vaults page or My Vault (Private) page and then click on the **Add** button to create a new entry.



Add a new Entry

Moving the mouse over the **Add** button will display a list of shortcuts for common entries.

Entries come in various types, all serving different purposes for your convenience.



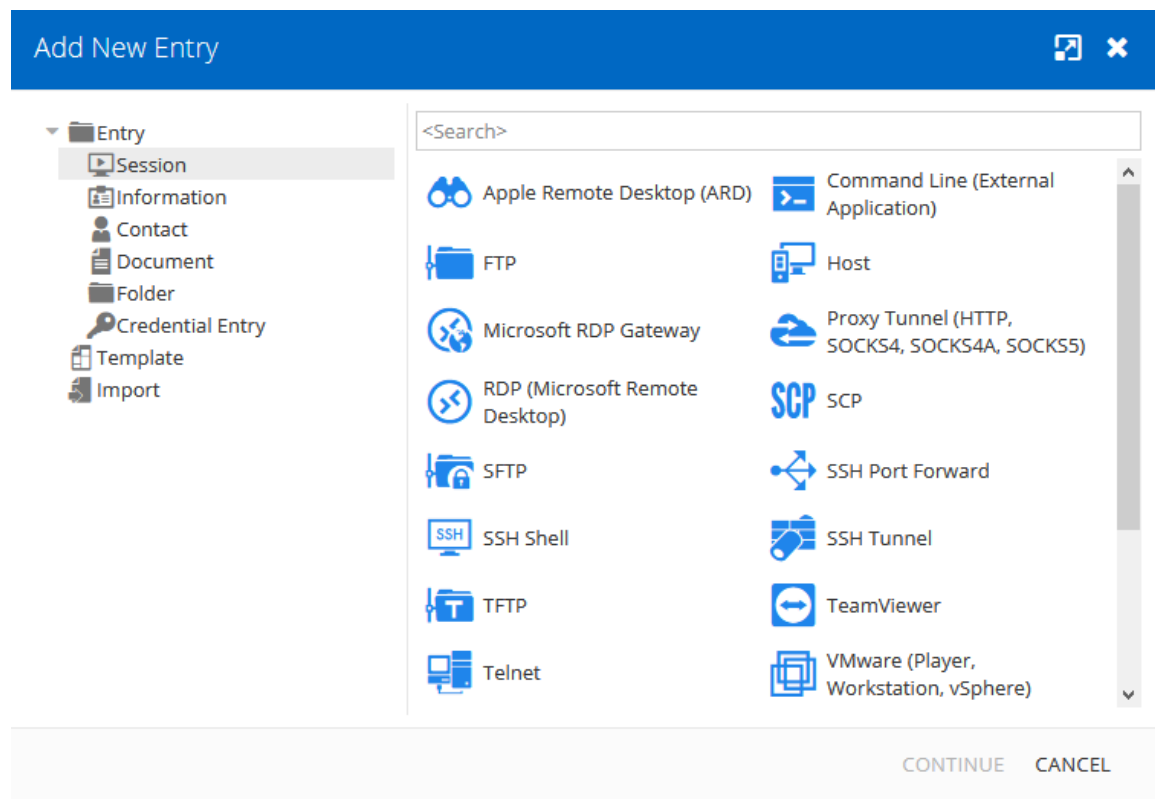
New Entry

OPTIONS	DESCRIPTION
Session	Session type entries are used for connections.
Information	Information type entries are used to store all sorts of data, both sensitive or not.
Contact	Contact type entries are used to store information about particular individuals.
Document	Document type entries are used to store external files.
Folder	Folder entries are used to help you customize and compartmentalize your entries.
Credential Entry	Credential entries are used to store all sorts of credentials.

5.3.2.1 Session

DESCRIPTION

Session entry types are used to establish connections. Entries such as our RDP (Microsoft Remote Desktop) entry can be used to store credentials (or acquire those from credential entries) and can be used in a variety of ways.



Add a New Session Entry

5.3.2.1.1 RDP (Microsoft Remote Desktop)

DESCRIPTION

GENERAL

RDP (Microsoft Remote Desktop) - General

OPTION	DESCRIPTION
Host (Computer)	Enter the host name or IP address of the remote computer.
Port	Click on the link to modify the port number. Set the port to 0 to use the default port.
RDP Type	Select the RDP session type. Select between: <ul style="list-style-type: none"> • Normal • Azure Cloud Services

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Hyper-V (embedded only)
Username	Enter the username to connect to the remote computer.
Domain	Enter the domain to connect to the remote computer.
Password	Enter the password to connect to the remote computer.
Password Analyzer	Indicates the strength of the password.
Always ask password	Always ask password when connecting to the remote computer.
Open console (Admin mode)	Connect to the console session of a server using Remote Desktop for Administration. Normally required for TS Session Hosts only.

DISPLAY

RDP (Microsoft Remote Desktop)

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

DISPLAY

Remote Desktop Size

Remote Desktop Size: Default

☐ Center on screen

Custom width: 0

Custom height: 0

Screen sizing mode: Default

☐ Span on multiple screens if possible

☐ Use all my monitors for the remote session

☐ Use advanced location (winposstr)

Colors

Colors: Highest Quality (32 bits)

☒ Display the connection bar when in full screen mode

☒ Connection bar pinned (full screen)

[> LOCAL RESOURCES](#)

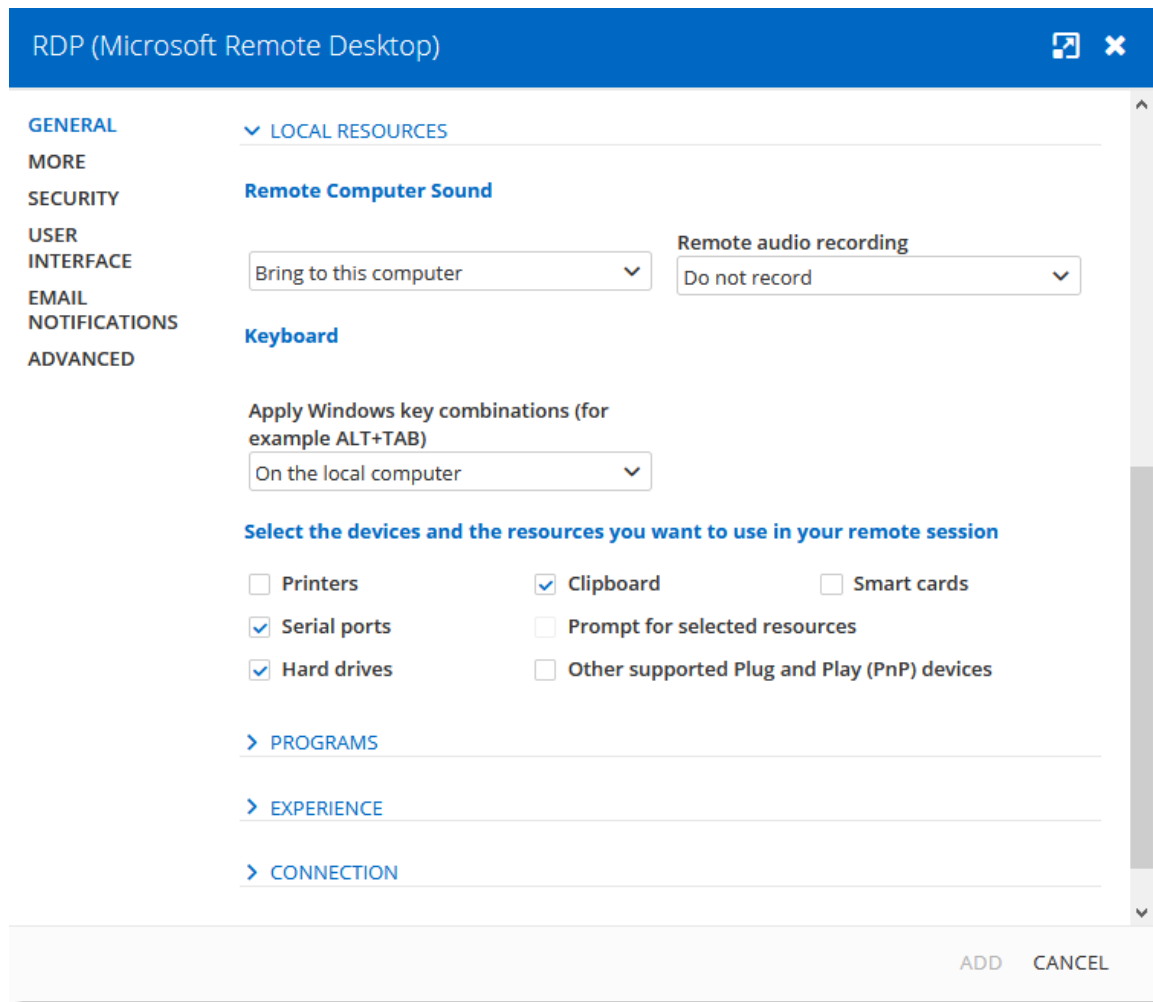
ADD CANCEL

RDP (Microsoft Remote Desktop) - Display

OPTION	DESCRIPTION
Remote Desktop Size	Select the screen size for the remote computer.
Custom width	Specify a custom width number for the screen size.
Custom height	Specify a custom height number for the screen size.
Screen sizing mode	Scale the client window display of the desktop when resizing between:

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Scrollbar.• Smart reconnect (reconnect the session when the window size changes).• Smart sizing (stretch the remote display to fit the window).
Colors	Select the color quality when connected on the remote computer.
Display the connection bar when in full screen mode	Display the connection bar at the top of your screen in full screen size mode.
Connection bar pinned (full screen)	Fix the connection bar at the top of the screen.

LOCAL RESOURCES



RDP (Microsoft Remote Desktop) - Local Resources

OPTION	DESCRIPTION
Remote computer sound	<p>Indicate what to do with the sound on the remote computer. Select between:</p> <ul style="list-style-type: none"> • Bring to this computer • Do not play • Leave at remote computer
Remote audio recording	<p>Indicate what to do with the audio recording on the remote computer. Select between:</p>

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Do not record• Record from this computer
Keyboard	<p>Specify how key combination should be executed. Select between:</p> <ul style="list-style-type: none">• On the local computer• On the remote computer• In full screen mode only
Select the devices and the resources you want to use in your remote session	<p>Select the devices and resources that you wish to use on the remote computer. Select between:</p> <ul style="list-style-type: none">• Printers• Serial Ports• Hard drives• Clipboard• Prompt for selected resources (Only available in external mode)• Other supported Plug and Play (PnP) devices• Smart cards

PROGRAMS

RDP (Microsoft Remote Desktop)

GENERAL > GENERAL

MORE > DISPLAY

SECURITY > LOCAL RESOURCES

USER INTERFACE > PROGRAMS

EMAIL NOTIFICATIONS

ADVANCED

☐ Start this program on connection (alternate shell)

Program path and filename Start in the following folder

☐ Use RemoteApp (seamless mode)

Program Parameters

☐ Execute the following program after login After login delay

> EXPERIENCE

> CONNECTION

> ADVANCED

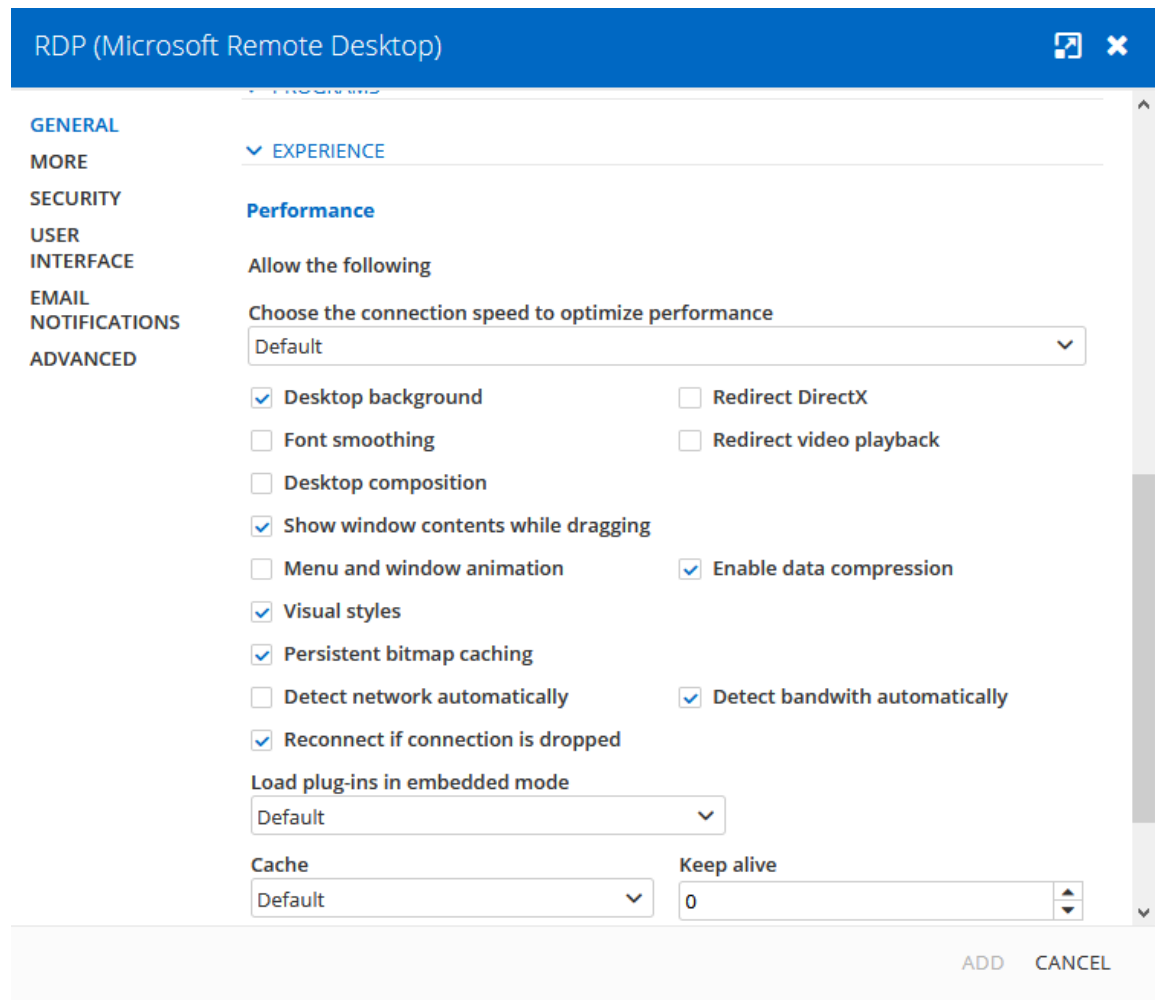
ADD CANCEL

RDP (Microsoft Remote Desktop) - Programs

OPTION	DESCRIPTION
Start the following program on connection (alternate shell)	Enable to specify a program to launch on the remote computer when the connection is established.
Program path and filename	Specify the program path and filename to start when the connection is established.
Start in the following folder	Specify the working folder used by the program in the previous step.

OPTION	DESCRIPTION
Use RemoteApp (seamless mode)	Open an rdp connection, starts a specified program, maximizes the application window and runs without the windows desktop.
Program	Specify the program for the RemoteApp.
Parameters	Specify the parameters for the RemoteApp.
Execute the following program after login	Enable if you wish to automatically run a program immediately after login.

EXPERIENCE



RDP (Microsoft Remote Desktop) - Experience

OPTION	DESCRIPTION
Choose the connection speed to optimize performance	<p>Specify the connection speed to use to optimize the remote session performance. Select between:</p> <ul style="list-style-type: none"> • Default • Modem (56 kbps) • Low-speed broadcast (256 kbps - 2 Mbps) • Satellite (2-16 Mbps with high latency)

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• High-speed broadcast (2-10 Mbps)• WAN (>10 Mbps with high latency)• LAN (> 10 Mbps with low latency)
Allow the following	<p>Enable the following features on the remote computer:</p> <ul style="list-style-type: none">• Desktop background• Font smoothing• Desktop composition• Show window contents while dragging• Menu and window animation• Visual styles• Persistent bitmap caching• Redirect DirectX• Redirect video playback• Load plug-ins in embedded mode• Enable data compression• Detect network automatically• Detect bandwidth automatically• Reconnect if connection is dropped
Cache	<p>Select the type of cache that will be used for the remote session:</p>

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Default: Use the value set in File – Options – Type – RDP – Cache.• Full mode: This protocol is full Windows 8 Remote Desktop protocol.• Thin client: This protocol is limited to using the Windows 7 with SP1 RemoteFX codec and a smaller cache. All other codecs are disabled. This protocol has the smallest memory footprint.• Small cache: This protocol is the same as Full mode, except it uses a smaller cache.
Keep alive	Data will be sent to the remote computer to keep the session alive. You can determinate the time between that and when the data is send. This option is only available in embedded mode.

CONNECTION

RDP (Microsoft Remote Desktop)

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

CONNECTION

Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy.

If the actual verification does not meet minimum policy requirements

Connect and don't warn me

☒ Activate network level authentication NLA (SingleSignOn)

☒ Automatically detect RD Gateway server settings

☐ Use these RD Gateway server settings:

Server name

Logon method

Allow me to select later

Gateway access token

☐ Open gateway only when unable to ping host

☐ Bypass RD Gateway server for local addresses

☐ Use same RD Gateway credentials as remote computer

Do not use RD Gateway server

ADD CANCEL

RDP (Microsoft Remote Desktop) - Connection

OPTION	DESCRIPTION
Server authentication verifies that you are connecting to the intended remote computer.	<p>If the actual verification does not meet minimum policy requirements, select what needs to be done by the remote computer between the following:</p> <ul style="list-style-type: none">• Connect and don't warn me• Do not connect• Warn me

OPTION	DESCRIPTION
Activate network level authentication (SingleSignOn)	Network Level Authentication completes user authentication before you establish a remote session and the logon screen appears. This is a more secure authentication method.
Automatically detect RD Gateway server settings	The RD Gateway server settings will be detected by the application automatically.
Use these RD Gateway server settings	Indicate the specific settings to connect on the RD Gateway server.
Server Name (Host)	Enter the RD Gateway server/host name.
Logon method	Select the logon method between: <ul style="list-style-type: none">• Ask for password (NTLM)• Smart card• Allow me to select later• Use a gateway access token
Gateway access token	Provide the access token if the Logon method is set to Use a gateway access token.
Open gateway only when unable to ping host	Establish a connection with the RD Gateway server only when it is not possible to ping the remote computer.
Bypass RD Gateway server for local addresses	Bypass the RD Gateway server when connecting on a remote computer who has a local IP address.
Use same RD Gateway credentials as remote computer	Use your personal RD Gateway credentials to connect on the remote computer.

OPTION	DESCRIPTION
Credentials	See RDP Gateway credentials section below.
Do not use RD Gateway server	Don't use any RD Gateway server to connect on the remote computer.

RDP GATEWAY CREDENTIALS

RDP Gateway Credentials

☒ Use custom credentials

Username

Domain

☒ Store password on the local computer

☐ Store password in the database

Password

.....

...

☐ Use credential repository

Select Credentials

▼

☐ Use my personal credentials

☐ Use private vault search

Search string

OK

CANCEL

RDP (Microsoft Remote Desktop) - Gateway Credentials

OPTION	DESCRIPTION
Use custom credentials	Use a specific username, domain and store the password on the local computer or store the password in the database.
Store password on the local computer	<p>This will use the Windows Credential Manager. It is not the best option because it has the following limitations:</p> <ul style="list-style-type: none">• The Credential Manager will hold only one entry per host, therefore if you have multiple sessions towards the same host, the last saved entry will overwrite whatever was stored.• The one host limitation ignores the port, therefore multiple sessions towards the same host, but with different ports, will conflict as well. Last saved entry overrides whatever was stored.
Store password in the database	The password will be store in the database.
Use Credential repository	Use a linked credential entry.
Use my personal credentials	Use the credentials stored in My Personal Credentials .
Use Private Vault search	Use the Search string to search for credential entries in the Private Vault.

ADVANCED

RDP (Microsoft Remote Desktop)

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

CONNECTION
ADVANCED

Enable CredSSP support
Default

Log off mode
Default

Automatically logoff when disconnecting
Default

Reconnect mode
Standard

RDP Version 7
Latest

Minimal input send interval
100 ms

☐ Use Thinstuff TSX Connection client
☐ Background input
☐ Enable super pan
☐ Public mode
☐ Restricted admin mode

Connection Broker - High Availability

Workspace ID
☐ Use redirection server

Alternate full address
Load balance info

ADD CANCEL

Microsoft Remote Desktop - (RDP) - Advanced

OPTION	DESCRIPTION
Enable CredSSP support	RDP will use the Credential Security Support Provider (CredSSP) for the authentication on the remote computer. Select between:
Log off mode	Select the log off method between: <ul style="list-style-type: none"> • Default • Automatic • RDM Agent

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Remote Desktop Services API• Macro
Automatically logoff when disconnecting	Automatically log off your RDP session when disconnecting.
Reconnect mode	Select the reconnect behavior. Select between: <ul style="list-style-type: none">• Default• Full• Smart reconnect• Legacy
RDP Version	Select the Remote Desktop Protocol version.
Minimal input send interval	Set the minimum time in milliseconds between the input is send to the remote computer.
Background input	The remote computer can accept input even when the focus is not on the session.
Restricted admin mode	This enables the restricted admin mode.
Enable super pan	Enabling super pan will take the entirety of your screen for the RDM session.
Public mode	Public mode is a security feature that limits the security information stored on the remote station. It also limits the amount of time this information can be stored.
Workspace ID	Enter the Workspace ID that contain the setting associate to the RemoteApp and Desktop ID.
Use redirection server	Redirect a remote computer to the RDP session host.

OPTION	DESCRIPTION
Alternate full address	Indicate an alternate name of the remote computer that you want to connect on.
Load balance info	Indicate the load balance info when the load balancing feature is enable on the RD Connection Broker.

5.3.2.1.2 Apple Remote Desktop (ARD)

DESCRIPTION

GENERAL (LOGON SETTINGS)

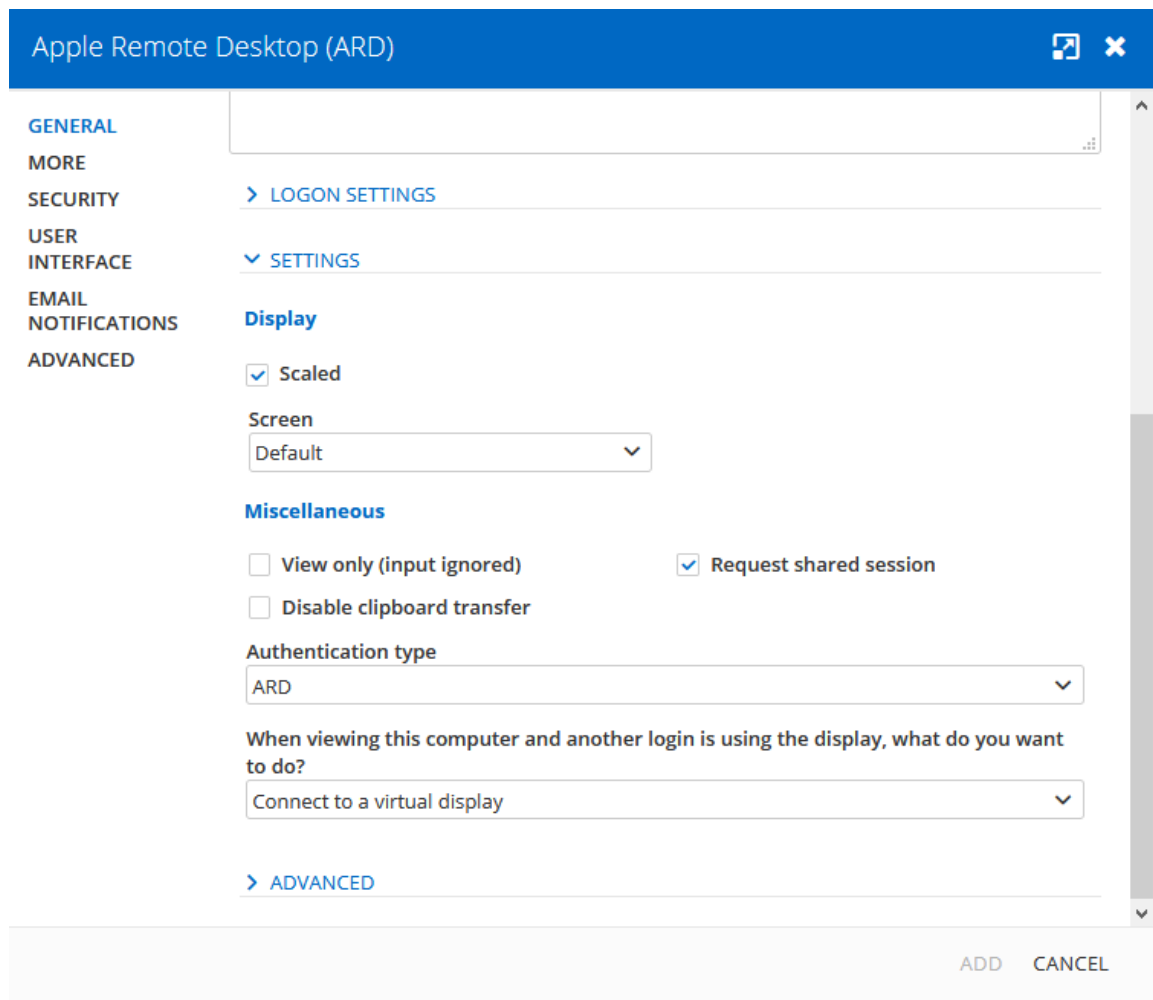
The screenshot shows the 'Apple Remote Desktop (ARD)' configuration window. The left sidebar contains a list of tabs: GENERAL (selected), MORE, SECURITY, USER INTERFACE, EMAIL NOTIFICATIONS, and ADVANCED. The main area is divided into sections. The 'GENERAL' section includes 'Display' (set to 'Embedded (tabbed)'), 'Monitor' (set to 'Primary monitor'), 'Credentials' (set to 'Default'), and a 'Description' text area. Below this is a section titled 'LOGON SETTINGS' which contains fields for 'Host', 'Port' (set to 5900 with a 'Default port' button), 'Username', and 'Password' (masked with dots). At the bottom of the main area are links for 'SETTINGS' and 'ADVANCED'. The bottom of the window has 'ADD' and 'CANCEL' buttons.

Apple Remote Desktop - General

OPTION	DESCRIPTION
Host	Enter the host name or IP address of the remote device.
Port	Enter the port to access the remote computer. Set the value to 0 to use the default port.
Username	Enter the username to connect to the remote computer.
Password	Enter the password to connect to the remote computer.

OPTION	DESCRIPTION
Password Analyzer	Indicates the strength of the password.

SETTINGS



Apple Remote Desktop - Settings

OPTION	DESCRIPTION
Scaled	Scale the remote display to fit the window.

OPTION	DESCRIPTION
Screen	<p>Select the screen where you want to display the remote connection. Select between:</p> <ul style="list-style-type: none">• Default: Use the setting in <i>File – Options – Types – Others – Apple Remote Desktop (ARD)</i>.• Primary: Display the primary screen.• Custom: Select which screen to display.• Prompt: Prompt at opening to select the remote display if there is more than one.
View only (input ignored)	<p>Connect in view only mode. This option disables the keyboard and mouse while in session.</p>
Request shared session	<p>The remote user will be prompted with a request to share his session.</p>
Disable clipboard transfer	<p>Disable the clipboard sharing.</p>
Authentication type	<p>Select the authentication mode for the connection. Select between:</p> <ul style="list-style-type: none">• ARD• ARD ask observe• ARD ask control

ADVANCED

Apple Remote Desktop (ARD)

GENERAL
MORE
SECURITY
USER
INTERFACE
EMAIL
NOTIFICATIONS
ADVANCED

Description

[LOGON SETTINGS](#)

[SETTINGS](#)

▼ [ADVANCED](#)

Mouse

Mouse cursor
Track remote cursor locally
☒ Emulate 3 buttons (with 2-button click) ☐ Swap mouse buttons 2 and 3
Keyboard

Apply Windows key combinations (for example ALT+TAB)
On the local computer
Encoding

Preferred encoding
Default

ADD CANCEL

Apple Remote Desktop - Advanced

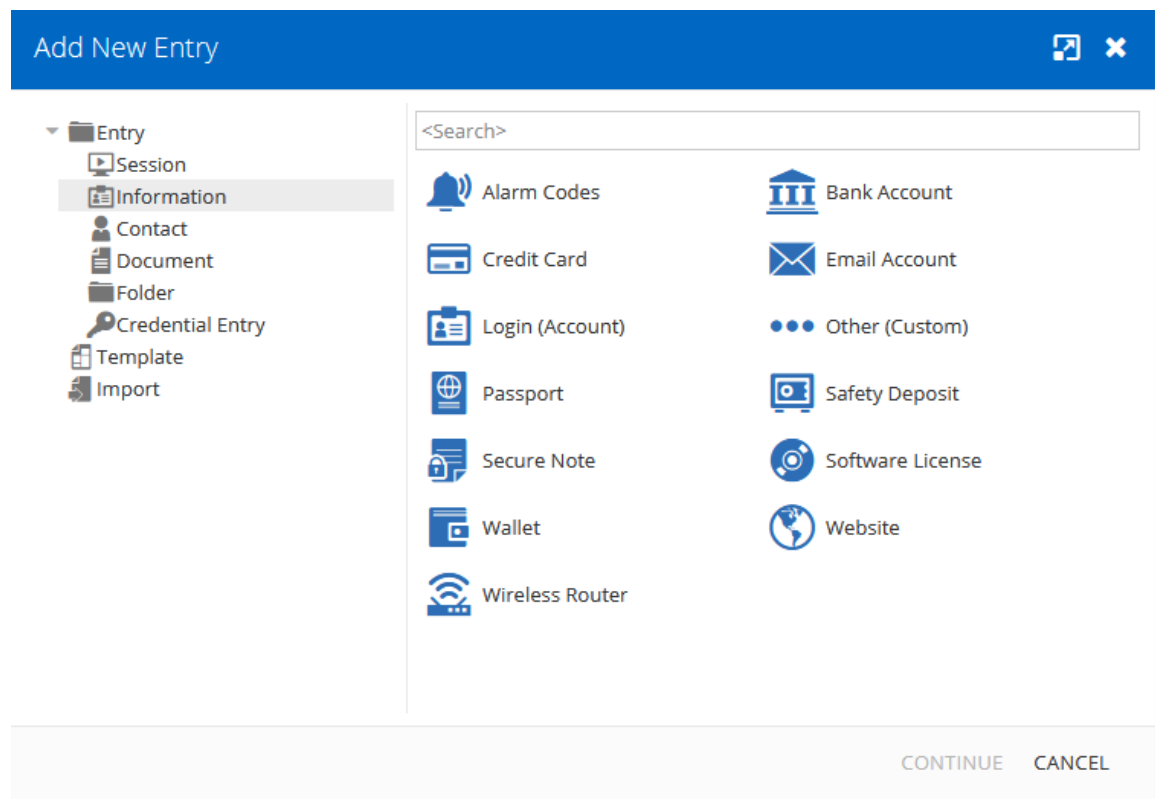
OPTION	DESCRIPTION
Mouse cursor	Select the way the mouse cursor is handled. Select between: <ul style="list-style-type: none">• Track remote cursor locally• Let remote server deal with mouse cursor• Don't show remote cursor
Emulate 3 buttons (with 2-button click)	Emulate mouse button 3 when clicking on both button 1 and button 2.

OPTION	DESCRIPTION
Swap mouse buttons 2 and 3	Invert mouse buttons 2 and 3.
Apply Windows key combinations	Select where the key combinations are sent. Select between: <ul style="list-style-type: none">• On the local computer• On the remote computer• In full screen mode only
Keyboard layout	Select the keyboard layout. Select between: <ul style="list-style-type: none">• Azerty• Qwerty
Preferred encoding	Change the encoding to use less bandwidth. From the least to the most bandwidth used, select between: <ul style="list-style-type: none">• Zlib 16 gray (black and white)• Zlib halftone (black and white)• Zlib thousands (in color)• Zlib (you can choose your custom compression level)• Default (color)

5.3.2.2 Information

DESCRIPTION

Information entry types are used to store sensitive information like alarm codes, serial numbers, credit card information and more into the data source.



Add a new Information Entry

5.3.2.2.1 Alarm Codes

DESCRIPTION



The **Alarm Codes** entry is used for securely storing employee/alarm code pairings.

GENERAL

Click on the **General** side menu and enter a Name for your newly created entry, then click on the **plus sign** to add information.

Information - Alarm Codes

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

Name *

The name is required.

Folder

Vault (Windjammer IT)

Display

Embedded (tabbed) ▼

Monitor

Primary monitor ▼

Description

Image

Alarm Codes

No data to display

ADD

CANCEL

Information Entry - Alarm Codes

SETTINGS

Enter all the Alarm Codes information and then click on **OK** to add it to your entry. You can add multiple Alarm codes to the same entry, once you've entered all the Alarm codes simply click on **Add**.

Information - Alarm Code

Employee

Stan

Alarm code

.....

☒ Is hidden

Employee code

1234

Note

Alarm code for May 2018

OK

CANCEL

New Alarm Code

OPTION	ENCRYPTED	DESCRIPTION
Employee		Enter the employee's name.
Alarm code	✓	Enter the alarm code.
Employee code		Enter the employee's code.
Note		Add a note regarding the alarm code.

5.3.2.2.2 Email Account

DESCRIPTION



The **Email Account** entry is useful to securely store email account settings including POP3/IMAP/SMTP servers, username and passwords.

SETTINGS

GENERAL

Click on the **General** side menu and enter all the required information in the **General tab**. Once all required information in all tabs is entered click on **Add**.

The screenshot shows a window titled "Information - Email Account" with a blue header bar. On the left is a sidebar menu with the following items: GENERAL (highlighted in blue), MORE, SECURITY, USER, INTERFACE, and ADVANCED. The main area contains the following fields and controls:

- Name:** A text input field.
- Image:** A square area containing an email icon.
- Folder:** A text input field with "Private Vault" and a three-dot menu icon to its right.
- Display:** A dropdown menu showing "Embedded (tabbed)".
- Monitor:** A dropdown menu showing "Primary monitor".
- Description:** A large text area.
- Navigation links:** Four links with right-pointing chevrons: GENERAL, POP3, IMAP, and SMTP.

At the bottom right of the dialog are two buttons: "ADD" and "CANCEL".

Information Entry - Email Account - General Tab

OPTION	ENCRYPTED	DESCRIPTION
Your name		Enter the account name.
Email		Enter the email address.
S/MIME		Enable if this email account requires/uses Secure/Multipurpose Internet Mail Extensions.

POP3

Information - Email Account

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Display
Embedded (tabbed)

Monitor
Primary monitor

Description

▶ GENERAL

▼ POP3

Host NamePort

110

UsernamePassword

.....

☐ SSL 3.0

Authentication
Password

▶ IMAP

▶ SMTP

ADD CANCEL

Information Entry - Email Account - POP3 Tab

© 2020 Devolutions inc.

OPTION	ENCRYPTED	DESCRIPTION
Host name		Enter the POP3 host name.
Port		Enter the POP3 port, the default port is 110.
Username		Enter the POP3 username.
Password	✓	Enter the POP3 password.
SSL 3.0		Enable if the POP3 requires an SSL connection.
Authentication		Choose your POP3 authentication mode between: <ul style="list-style-type: none">• AppleToken• HTTPMD5Digest• MD5ChallengeResponse• NTLM• Password

IMAP

Information - Email Account

GENERAL

MORE

SECURITY

USER INTERFACE

ADVANCED

Display

Embedded (tabbed)

Monitor

Primary monitor

Description

GENERAL

POP3

IMAP

Host Name

Port

143

Username

Password

.....

SSL 3.0

☐

Authentication

Password

SMTP

ADD

CANCEL

Information - Email Account - IMAP Tab

OPTION	ENCRYPTED	DESCRIPTION
Host name		Enter the IMAP host name.
Port		Enter the IMAP port, the default port is 143.
Username		Enter the IMAP username.
Password	✓	Enter the IMAP password.
SSL 3.0		Enable if the IMAP requires an SSL connection.

OPTION	ENCRYPTED	DESCRIPTION
Authentication		<p>Choose your IMAP authentication mode between:</p> <ul style="list-style-type: none">• AppleToken• HTTPMD5Digest• MD5ChallengeResponse• NTLM• Password

SMTP

Information - Email Account

GENERAL
MORE
SECURITY
USER INTERFACE
ADVANCED

Description

GENERAL
POP3
IMAP
SMTP

Host Name
Port

☐ My outgoing server (SMTP) requires authentication
☐ Use same settings as my incoming mail server

Username
Password

☐ SSL 3.0

Authentication

ADD CANCEL

Information Entry - Email Account - SMTP Tab

OPTION	ENCRYPTED	DESCRIPTION
Host name		Enter the SMTP host name.
Port		Enter the SMTP port, the default port is 25.
My outgoing server (SMTP) requires authentication		Does the SMTP server require authentication.
Use same settings as my incoming mail		Use POP3 or IMAP settings for the outgoing server authentication.

OPTION	ENCRYPTED	DESCRIPTION
server		
Username		Enter the SMTP username.
Password	✓	Enter the SMTP password.
SSL 3.0		Enable if the SMTP requires an SSL connection.
Authentication		<p>Choose your SMTP authentication mode between:</p> <ul style="list-style-type: none"> • AppleToken • HTTPMD5Digest • MD5ChallengeResponse • NTLM • Password

5.3.2.2.3 Website

DESCRIPTION



The **Website** entry is useful for storing web site credential information including username, domain and password.

SETTINGS

Click on the **General** side menu and enter all the required information, then click on **Add**.

OPTION	ENCRYPTED	DESCRIPTION
		<ul style="list-style-type: none"> • Inherited: inherit the credentials from a parent folder. • None: do not provide any credentials in the entry. • Private Vault search: search for an existing credentials entry in the user's Private Vault. The exact name of the credential entry must be provided. If two matches occur, the user is prompted with all available credential entries in their Private Vault.
Username		Enter the username associated to the website's account.
Domain		Enter the domain associated to the website's account.
Password	✓	Enter the password associated to the website's account.

5.3.2.2.4 Note/Secure Note

DESCRIPTION



The **Note/Secure Note** entry is a simple free form note allowing you to securely store any type of free form information.

SETTINGS

Click on the **General** side menu and enter all the required information, you can choose between the HTML or plain text format, then click on **Add**.

Information - Secure Note

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Name

Folder
Private Vault

Display
Embedded (tabbed)

Monitor
Primary monitor

Description

Secure Note

☐ Is sensitive

HTML

Heading 1

B *I* U `<>` -

-

Link

ADD CANCEL

Information Entry - Note/Secure Note

5.3.2.3 Contact

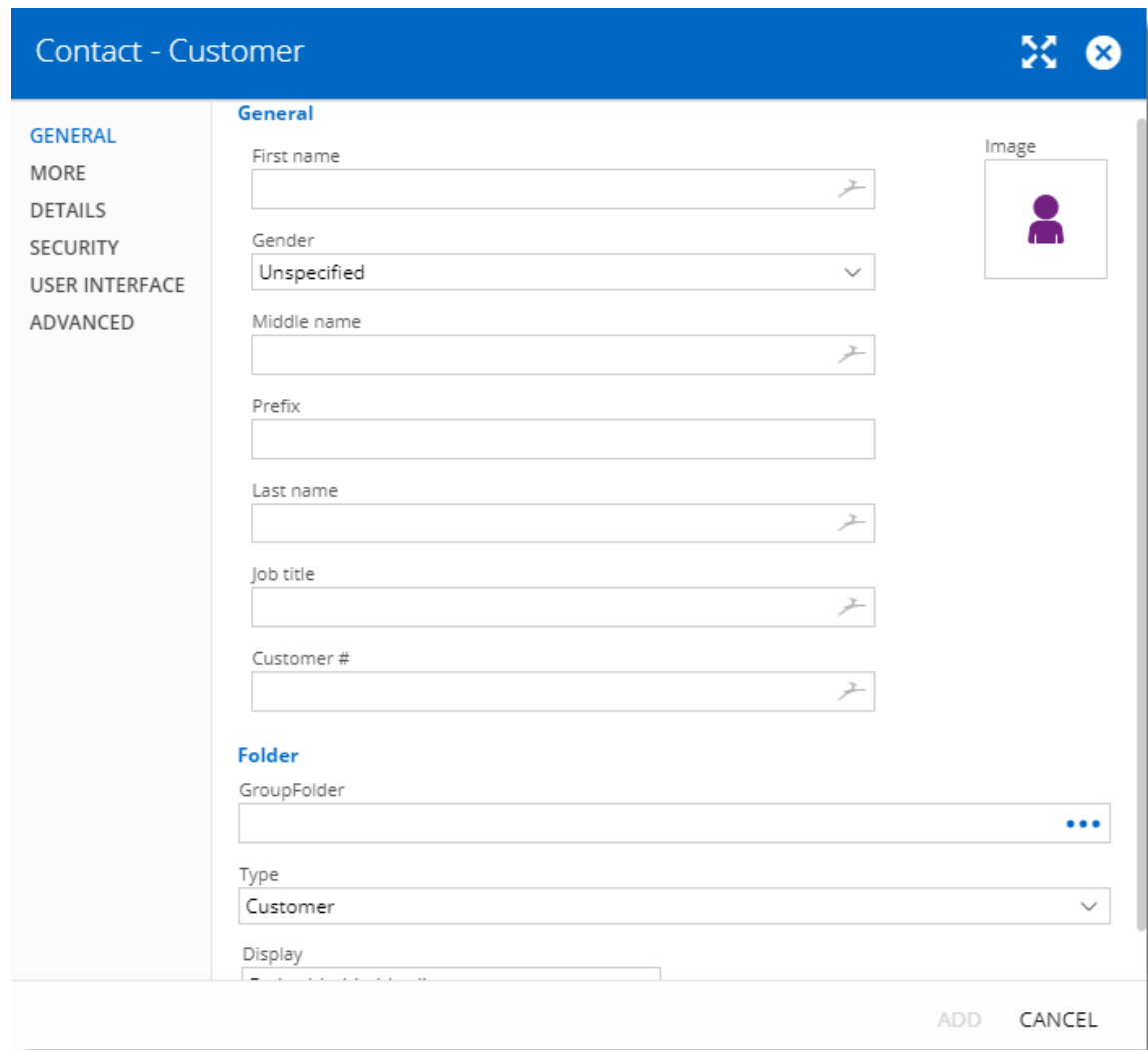
DESCRIPTION

Contact entry types are used to manage your contacts in Devolutions Server.

SETTINGS

GENERAL

Use the **General** side menu to enter basic information about the contact, such as their name, gender and job title.



The screenshot shows a web application window titled "Contact - Customer". On the left is a side menu with the following items: GENERAL (highlighted in blue), MORE, DETAILS, SECURITY, USER INTERFACE, and ADVANCED. The main area displays the "General" tab. It contains several input fields: "First name", "Gender" (a dropdown menu currently showing "Unspecified"), "Middle name", "Prefix", "Last name", "Job title", and "Customer #". To the right of these fields is an "Image" placeholder with a person icon. Below the main fields is a "Folder" section with "GroupFolder" (a text field with a blue ellipsis icon) and "Type" (a dropdown menu currently showing "Customer"). At the bottom of the form is a "Display" field. At the bottom right of the window are "ADD" and "CANCEL" buttons.

Contact Entry - Customer - General side Menu

DETAILS

Use the **Details** side menu to enter information about the contact's company address, email and phone number.

Contact - Customer

GENERAL
MORE
DETAILS
SECURITY
USER INTERFACE
ADVANCED

Address

Company

Address

City

State

Zip code

Country

United States

Email/Phones

Email

Home phone

Work phone

Mobile

Fax

Skype

Website

ADD CANCEL

Contact Entry - Customer - Details side Menu

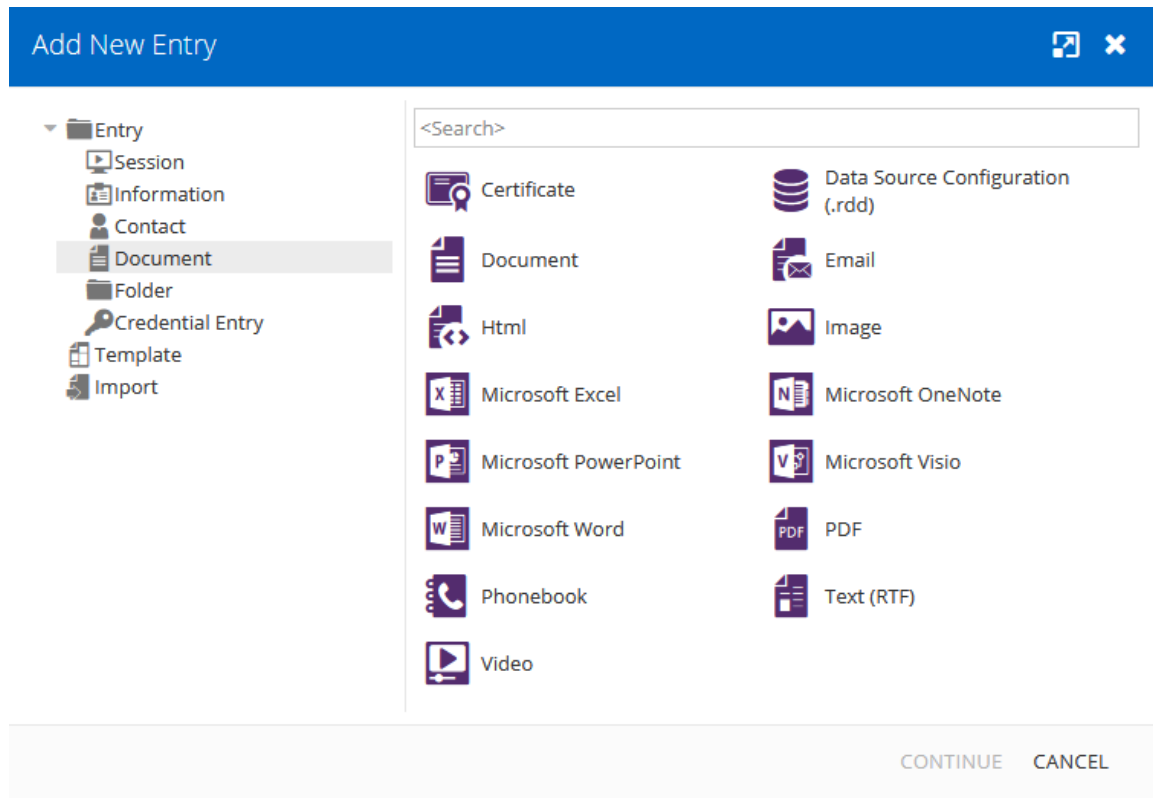
5.3.2.4 Document

DESCRIPTION

Document entry types are used to store any type of document directly in the data source.



For architectural reasons, the documents stored in our Advanced Data sources are **NOT** protected from deletions. Once they are deleted, **they cannot be restored**. Please keep a safe copy of all documents in another storage device. Support for this feature will be added in a coming update to our products.



Add a new Document Entry


SETTINGS

Document

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Name

Image



Folder

Private Vault

...

Description

Document

Mode

Stored in database

...

ADD CANCEL

Document Entry - Default

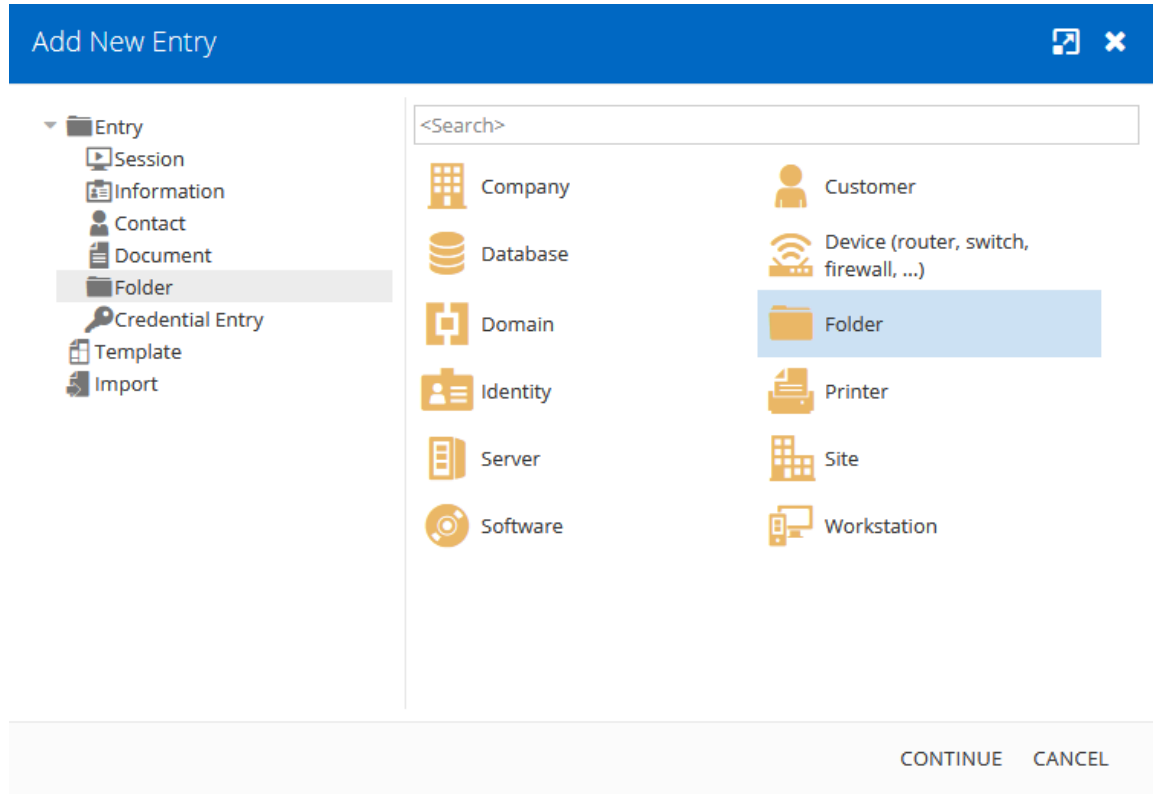
OPTION	ENCRYPTED	DESCRIPTION
File Type		Indicate the file type entry you wish to create.
Mode		Select the mode between: <ul style="list-style-type: none">• Stored in database (select a file stored in the database)• URL (open a file using a URL)

OPTION	ENCRYPTED	DESCRIPTION
Stored in database		If you have selected the Stored in database mode, click on the ellipsis in the box under to select a file that will be stored in the database. Some data sources do not support this mode.
URL		If you have selected the URL mode, click in the box under to enter the URL.

5.3.2.5 Folder

DESCRIPTION

Folders are used to organize your entries in a logical way. It is possible to create an extensive hierarchy of folders and sub folders, alphabetically sorted.



Folder Entry

SETTINGS

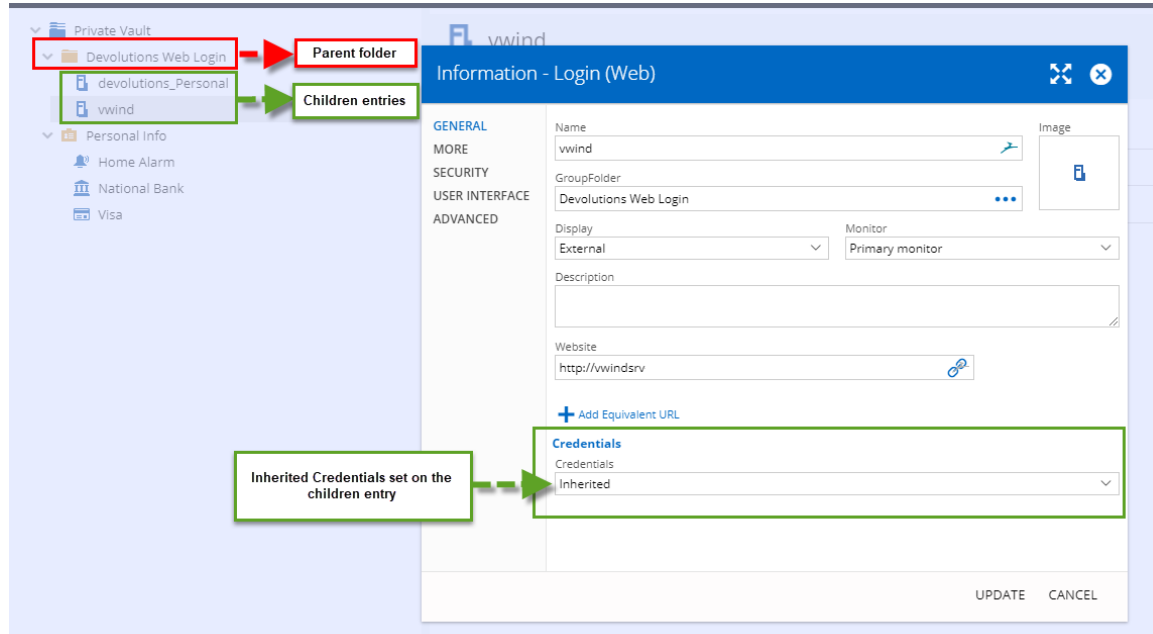
Enter a name for your **Folder**. You could also define a username, domain and password directly in your folder if you wish for the child entries to inherit from it.

The screenshot shows a settings window titled "Folder - Folder" with a blue header bar containing window control icons. On the left is a sidebar with menu items: GENERAL (highlighted in blue), MORE, SECURITY, USER INTERFACE, and ADVANCED. The main content area is divided into two sections. The top section, under the "GENERAL" tab, includes a "Name" text field, a "GroupFolder" dropdown menu currently showing "Devolutions Web Login" with a three-dot menu icon, a "Credentials" dropdown menu showing "Default", a "Description" text area, and two checkboxes: "Allow reveal credentials (everybody)" (unchecked) and "Allow add entry in group" (checked). To the right of these fields is an "Image" section with a folder icon. The bottom section, titled "DETAILS" with a dropdown arrow, contains a "Type" dropdown menu set to "Folder", and text fields for "Username", "Domain", and "Password". The "Password" field has an eye icon and a three-dot menu icon. At the bottom right of the window are "ADD" and "CANCEL" buttons.

Folder - Folder

INHERITED CREDENTIALS

If you want your child entries (meaning entries stored under your folder) to inherit the credentials set on the folder (also called parent folder), you must specify **Inherited** credentials in your child entries.



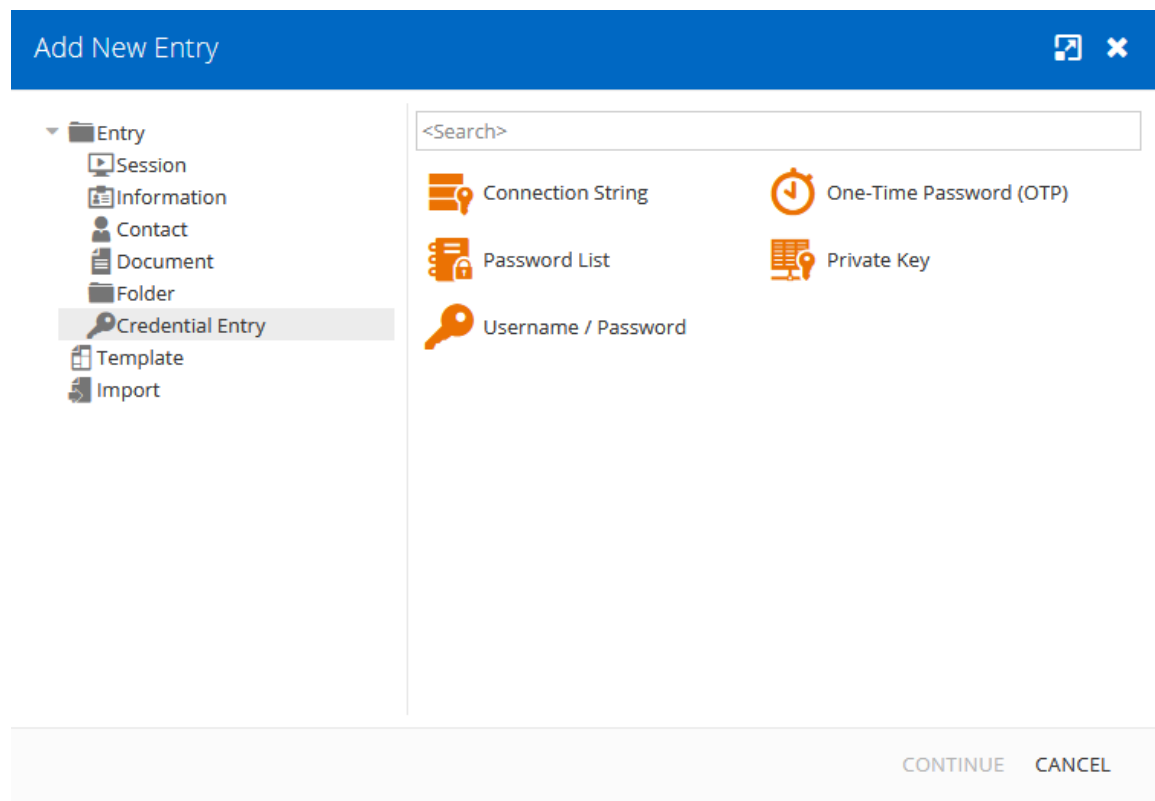
Inherited Credentials set on your child Entry

5.3.2.6 Credential Entry

DESCRIPTION

Credential entries are used to store account information, such as usernames, passwords, domains, etc. **Credentials** are available from the **credential repository**, a collection of all the credentials stored in the data source.

Credentials entries allows you to set multiple sessions to use specific credentials in the data source. This simplifies management by allowing you to maintain a single credential entry for multiple entries.



Add New Entry - Credential Entry

5.3.2.6.1 Connection String

DESCRIPTION



This entry is used to define and configure a **Connection String** credential entry.

SETTINGS

Credentials - Connection String

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Name

Folder
Private Vault

Description

GENERAL

Data source
Microsoft SQL Server

Data provider
.NET Framework Data Provider for SQL Server

Connection string
.....

Image

ADD CANCEL

Credentials - Connection String

OPTION	DESCRIPTION
Data Source	Contains data source types like ODB, OLEDB or native. This value is read only and is extracted from the connection string.
Data provider	Specify the provider used for the database access. This value is read only and is extracted from the connection string.
Connection String	This value contains the database connection string and it can be hidden/encrypted for a higher level of security
Eye/Lock button	Reveal or hide the connection string.

5.3.2.6.2 One-Time Password (OTP)

DESCRIPTION



This entry is used to define and configure a **One Time Password** credential entry.

SETTINGS

The **One Time Password** credential type is used as a second authentication factor that allows a user to secure their account with a generated verification code that changes over time.

Credentials - One-Time Password (OTP)

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Name

Folder

Private Vault

Description

Logon Settings

Key

.....

Time step

30

Code size

6 Digits

Hash algorithm

SHA-1

Image

ADD CANCEL

Credentials - One-Time Password

OPTION	DESCRIPTION
Key	Enter the secret key given by the website or the application.
Time step	Enter the amount of time for which the generated verification code is valid.
Code size	Select the amount of digits the generated verification code contains. Select between: <ul style="list-style-type: none">• 6 Digits• 8 Digits
Hash algorithm	Select the secure hash algorithm used to generate the verification code. Select between: <ul style="list-style-type: none">• SHA-1• SHA-256• SHA-512

ENABLING MULTIFACTOR AUTHENTICATION

To use the multifactor authentication, this feature must be enabled from the user's account of a service or website that supports multifactor authentication. Usually, you can find the multifactor authentication settings in the user account security preferences. The name of the feature should be similar to two-factor authentication, two-step verification or multifactor authentication.



When enabling multifactor authentication, a list of recovery codes might be generated by the website or application. Carefully store these in a safe place, these recovery codes will be useful if the user happens to lose the **One Time Password** entry.

5.3.2.6.3 Password List

DESCRIPTION



This entry is used to define and configure a **Password List** credential entry. **Password Lists** store multiple username and password entries in one entry, minimizing the number of entries in the Vault.

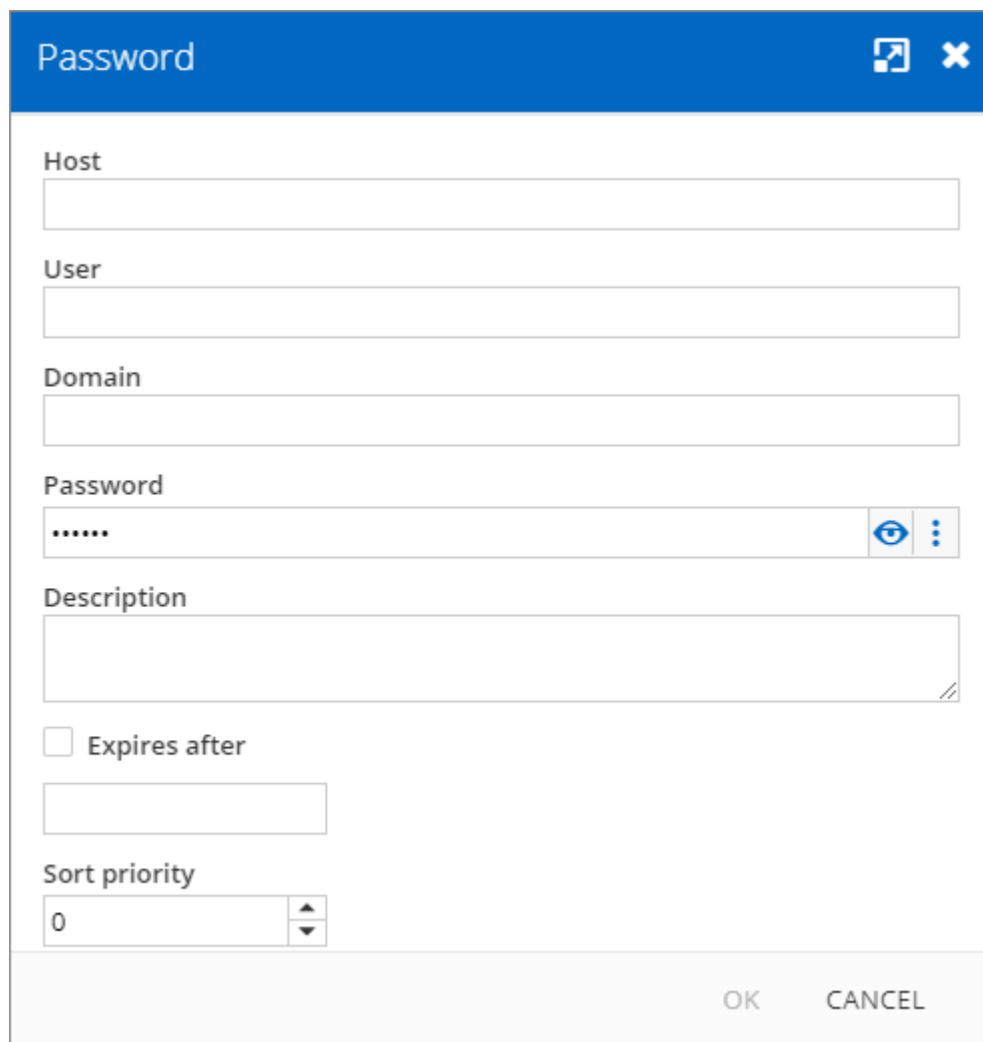
SETTINGS

Click the add button **+** to create a new password entry in the password list.

Password List Entry

ENTRIES IN THE PASSWORD LIST

The **Password** entry is created through the **Password List** entry.



The screenshot shows a dialog box titled "Password" with a blue header bar containing a maximize icon and a close button. The dialog contains several input fields: "Host", "User", "Domain", and "Password". The "Password" field is masked with dots and has a visibility toggle (eye icon) and a dropdown menu (three dots) to its right. Below these is a "Description" text area. Further down is a checkbox labeled "Expires after" followed by an empty input field. At the bottom is a "Sort priority" spinner control set to "0". The dialog has "OK" and "CANCEL" buttons at the bottom right.

Password List - Password

OPTION	DESCRIPTION
User	Enter a username.
Domain	Enter the domain name (optional).

OPTION	DESCRIPTION
Password	Enter the password.
Description	Enter a description (optional).
Expire	Select the Expire box to enter an expiration date for the password. Click the date box to choose an expiration date in the calendar.

5.3.2.6.4 Private Key

DESCRIPTION





This entry is used to define and configure a **Private Key** credential entry.

The **Private Key** entry uses an encrypted public/private key pair to authenticate a user on a remote device. The **Private Key** is a secure authentication approach as long as the **Private Key** remains secret.

SETTINGS

Private Key Entry - Properties

OPTION	DESCRIPTION
Private Key Type	Select between: <ul style="list-style-type: none"> • Data: the key is stored in the entry, accessible on any machine. • No private key: Does not send the private key (for advanced scenarios).
Passphrase	Enter the passphrase to unlock the private key.
Username	Enter the username associated with the private key.

OPTION	DESCRIPTION
Password	Not used under normal circumstances.
Private Key Data	Click the more button  to find a file and insert the private key data in the entry.
	Click to download the private key as a .ppk file.

GENERAL

ADVANCED

☐ Automatically load to key agent

Private Key Entry - Properties - Advanced

OPTION	DESCRIPTION
Automatically load to key agent	Automatically load the Private Key in the Key Agent Manager in Remote Desktop Manager.

5.3.2.6.5 Username/Password

DESCRIPTION



This entry is used to define and configure a **Username/Password** credential entry. This is the default credential type.

SETTINGS

Credentials - Username / Password

GENERAL
MORE
SECURITY
USER
INTERFACE
ADVANCED

Name

Image

Folder
Private Vault

Description

▼ GENERAL

Username

Domain

☐ Always ask password



Password

Mnemonic password

ADD CANCEL

Username / Password - Properties

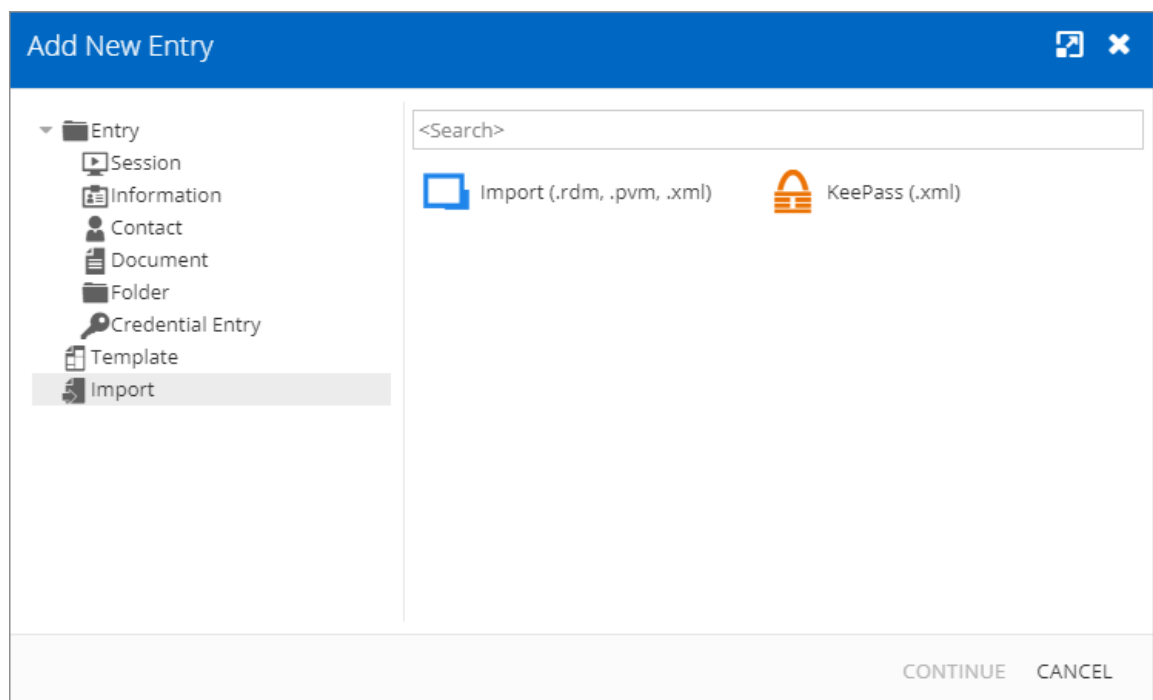
OPTION	DESCRIPTION
Username	Enter the username.
Domain	Enter domain.
Always ask password	Check box to prompt user for password each time they use the credential.

OPTION	DESCRIPTION
Password	<p>Enter the password.</p> <p>Click  to reveal the password.</p> <p>Click the advanced button  to generate a password or open the Password generator for more settings and password choices.</p>
Mnemonic password	<p>Enter a phrase to help remember the password.</p>

5.3.2.7 Import

DESCRIPTION

Use the **Import** selection to import entries in Devolutions Server. You can import entry types from a .RDM or from a KeePass file.

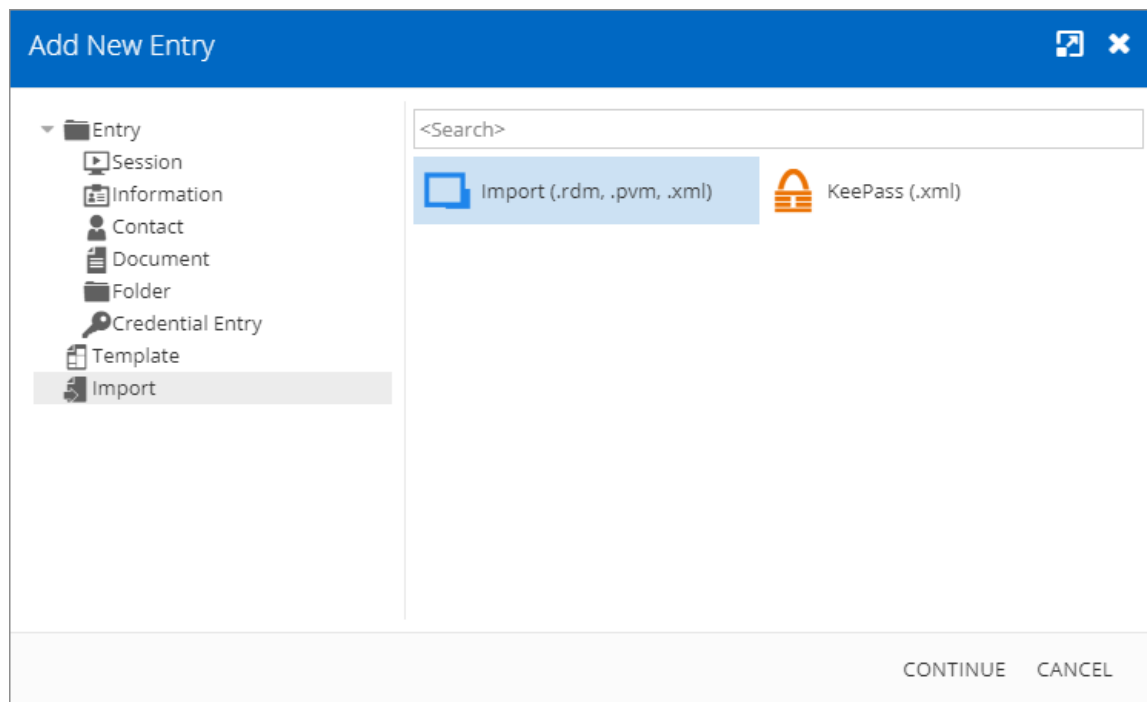


Add New Entry - Import

STEPS

Here are the steps to import entries from a file.

1. Select the file type, **Import (.rdm, .pvm, .xml)** or **KeePass (.xml)**, and then click on **CONTINUE**.



Add New Entry - Import

2. Select the file to import under **Select a file**.

The screenshot shows the 'Import Entries' dialog box with a blue header and three numbered steps: 1. File Selection, 2. Analyze, and 3. Import. Step 1 is active. Below the steps, there are three input fields: 'Select a File' with 'Entries.rdm' and a dropdown arrow, 'Import in folder' with 'Vault (Service Desk)' and a dropdown arrow, and 'Master key' with a masked password '.....' and a toggle icon. At the bottom right, there are buttons for 'BACK', 'NEXT', and 'CANCEL'.

Import Entries - File Selection

3. Select the destination folder under **Import in folder** if you want to import the entries under a specific folder. If no folder is selected, it will be automatically imported under **Root Folder**.

This screenshot shows the 'Import Entries' dialog box with the 'Folder' selection sub-dialog open. The sub-dialog has a blue header and a list of folders: 'Vault (Service Desk)', 'Non-Production' (with sub-folders 'General' and 'Orion.loc'), 'Production' (with sub-folders 'Confidential' and 'General'), and 'TestFolder'. The 'TestFolder' is highlighted. The sub-dialog has 'OK' and 'CANCEL' buttons at the bottom. The background dialog box shows the same fields as the previous screenshot, but the 'Import in folder' field now displays 'TestFolder'.

Import Entries - Folder Selection

4. Enter the password under **Master key** if the file is protected by a password. Then click on **Next**.

Import Entries

1 File Selection 2 Analyze 3 Import

Select a File
demo.rdm

Import in folder
TestFolder

Master key
.....

BACK NEXT CANCEL

Import - Entries - Master key

5. Select the operation for each entry. It is possible to set the operation for all entries with the **Apply All** button.

Import Entries

1 File Selection 2 Analyze 3 Import

Add ▼ Apply All

	Name	Entry Type	Folder
Add ▼	Downhill Pro	Group	Downhill Pro
Add ▼	UBUNTU-LAMP (H & T)	Host	Downhill Pro
Add ▼	Downhill DB 1	RDPConfigured	Downhill Pro
Add ▼	Downhill DC	RDPConfigured	Downhill Pro
Add ▼	Downhill Web 1	RDPConfigured	Downhill Pro
Add ▼	ladmin@downhill	Credential	Downhill Pro
Add ▼	RAS	Document	Downhill Pro

« < 1 2 3 4 5 > » 98 Results

BACK NEXT CANCEL

Import Entries - Analyze

6. Finally, click on the **Import** button to launch the import process.

Import Entries

1

2

3

File Selection

Analyze

Import

Action	Name	Entry Type	Group
Add	Downhill Pro	Group	Downhill Pro
Add	UBUNTU-LAMP (H & T)	Host	Downhill Pro
Add	Downhill DB 1	RDPConfigured	Downhill Pro
Add	Downhill DC	RDPConfigured	Downhill Pro
Add	Downhill Web 1	RDPConfigured	Downhill Pro
Add	ladmin@downhill	Credential	Downhill Pro
Add	RAS	Document	Downhill Pro
Add	vpn	VPN	Downhill Pro
Add	Microsoft RDP	RDPConfigured	Downhill Pro\UBUNTU-LAMP ...

BACK

IMPORT

CANCEL

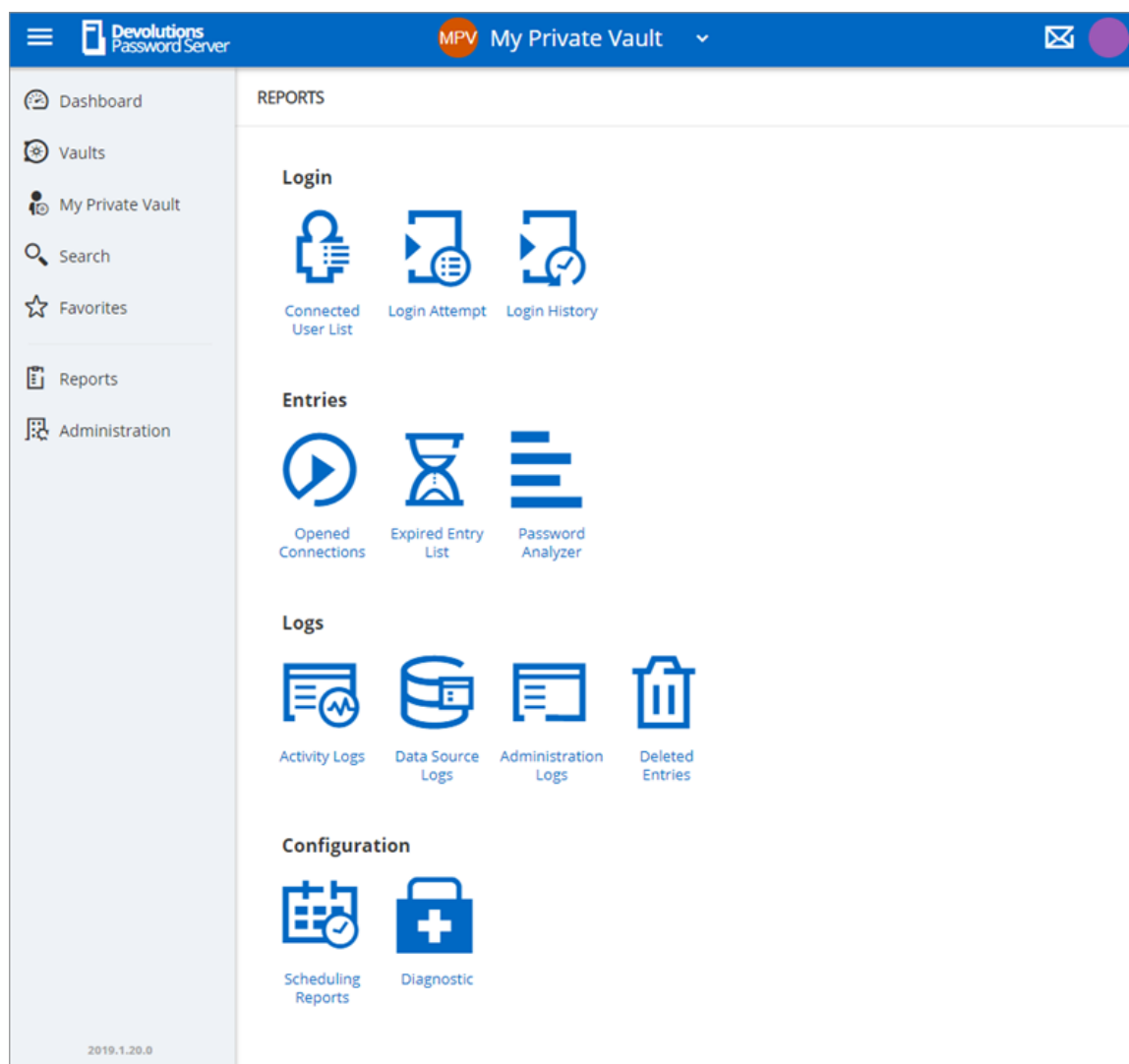
Import Entries - Import

5.4 Reports

DESCRIPTION

The **Reports** is only available for administrators. It allows the administrator to consult different reports.

REPORTS

*Reports*

OPTION	DESCRIPTION
Connected User List	This displays the users that are currently connected to the Devolutions Server data source.
Login Attempt	This lists all unsuccessful logins to the Devolutions Server data source.
Login History	The displays the information of each user that has been connected to the Devolutions Server data source.

OPTION	DESCRIPTION
Opened Connections	This lists all connections that are currently opened by users.
Expired Entry List	This displays the entries that are expired or should expire in the future.
Password Analyzer	This lists all entries containing encrypted passwords and displays their Strength.
Activity Logs	The displays the information about session activity.
Data Sources Logs	This displays the logs of the Devolutions Server data source.
Administration Logs	This displays the Admin logs of the Devolutions Server data source.
Deleted Entries	This lists every entries deleted in the data source.
Scheduling Reports	With this feature, you can set dates, filters and various customized settings to schedule recurring reports over any desire period.
Diagnostic	This will present a data source diagnostic report.

REPORT CUSTOMIZATION

Most of the reports available can be customized. It is possible to filter or sort the data, choose specific columns or even export the report in a .CSV file.

FILTERING AND SORTING

In front of the column title, the **filter button** offers some built-in filter values.

REPORTS > LOGIN HISTORY

Column Chooser

Username	Creation Date	Last update date	Token expiration date	Source	Platform
david@windjammer.loc	10/29/2019 09:35	10/29/2019 09:35	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/29/2019 09:20	10/29/2019 09:20	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/29/2019 13:51	10/29/2019 13:51	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/28/2019 13:21	10/28/2019 13:21	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/24/2019 13:57	10/24/2019 13:57	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/24/2019 12:53	10/24/2019 12:53	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/24/2019 10:07	10/24/2019 10:07	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/24/2019 10:04	10/24/2019 10:04	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/23/2019 15:17	10/23/2019 15:17	10/29/2019 11:04	Web	Web
david@windjammer.loc	10/22/2019 14:44	10/22/2019 14:44	10/29/2019 11:04	Web	Web

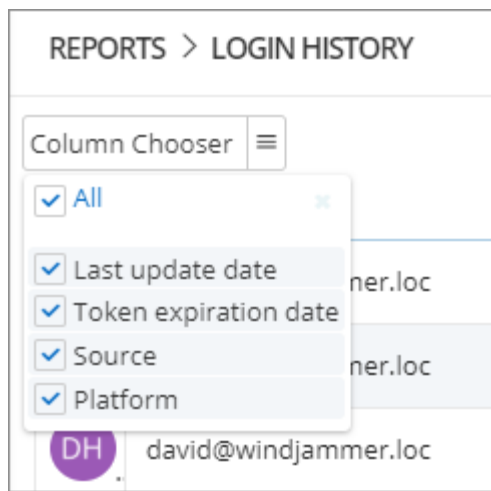
Export

10 Results

Filtering and Sorting Reports

COLUMN CHOOSER

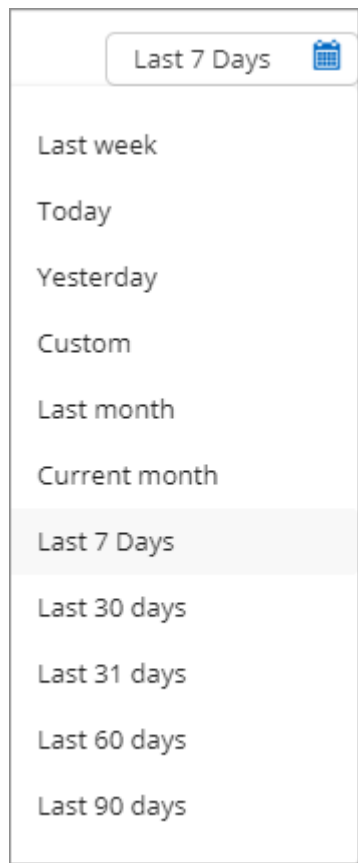
The **Column Chooser** button allows to select which columns will be displayed in the report.



Column Chooser selection Menu

TIME INTERVAL

Select the **Time Interval** on which the report will be based on.



Time Interval button

5.4.1 Configuration

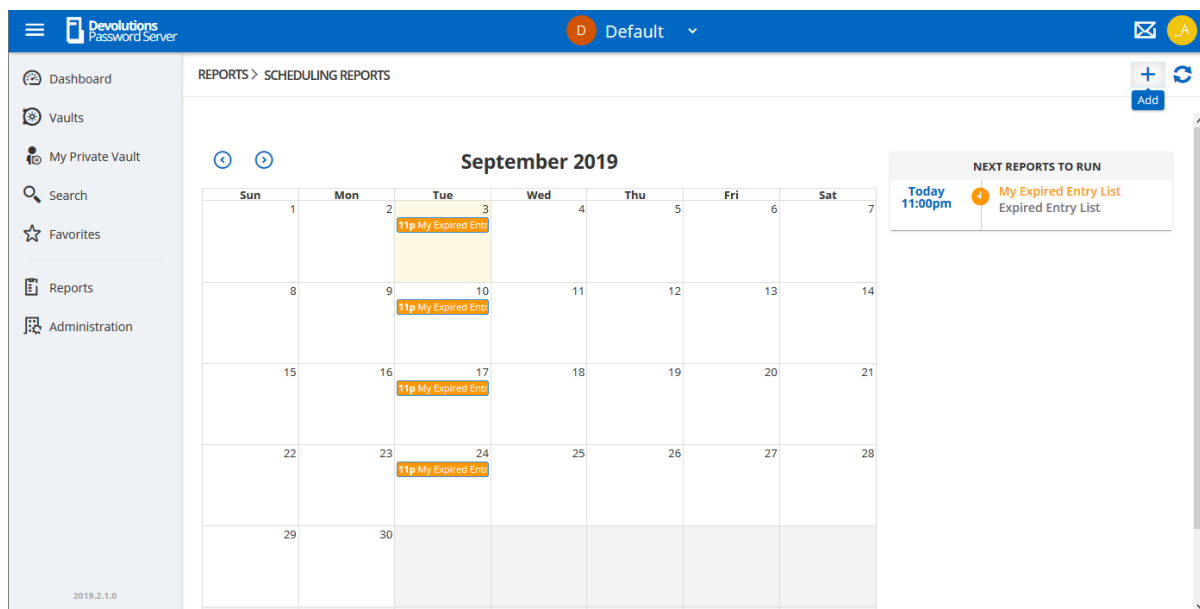
5.4.1.1 Scheduling Reports

DESCRIPTION

The Scheduling Reports will generate a report and send it by email to any selected user accounts. It could be an on demand report or a recurrent report based on a schedule (daily, weekly, monthly, yearly).

Only the Expired Entry List can be generated from the Scheduling Reports feature.

SETTINGS



Reports - Scheduling Reports

To create a new Scheduling Report, click on the Add button.

Event

General

Expired Entry List

Recipients

_administrator

Title

My Expired Entry List

Start

09/03/2019 23:00

Filter

☒ Include expired

☒ Include manually flagged expired

Expiring in 7 day(s)

Recurrence

☒ Recurrence

☐ Daily

Every 1 Week(s)

☒ Weekly

☐ Monthly

☐ Yearly

☐ End by

09/30/2019

☐ End after

4 occurrences

☒ No end date

SAVE

CANCEL

Scheduling Report creation

General options

OPTIONS	DESCRIPTION
Report type	Select the report type that will be generated. Only the Expired Entry List can be generated.
Recipients	Select all user accounts that will receive the report.
Title	Set the title of the report.

OPTIONS	DESCRIPTION
Start	Set the date and time when the report will be created.

Filter options

OPTIONS	DESCRIPTION
Include expired	Select this option to get all entries that are already expired in the report.
Include manually flagged expired	Select this option to get all entries that have been manually set to expire in the report.
Expiring in ... days	Set this option to get all entries that will expire in X days in the report.

Recurrence options

OPTIONS	DESCRIPTION
Daily, Weekly, Monthly, Yearly	Set the recurrence for this report.
Every ...	Set the the number for the recurrence.
End by	Set this option and the date to stop the report at a specific moment.
End after ... occurrences	Set this option to run this report a specific number of times.
No end date	Set this option to get the report running indefinitely.

5.4.1.2 Diagnostic

DESCRIPTION

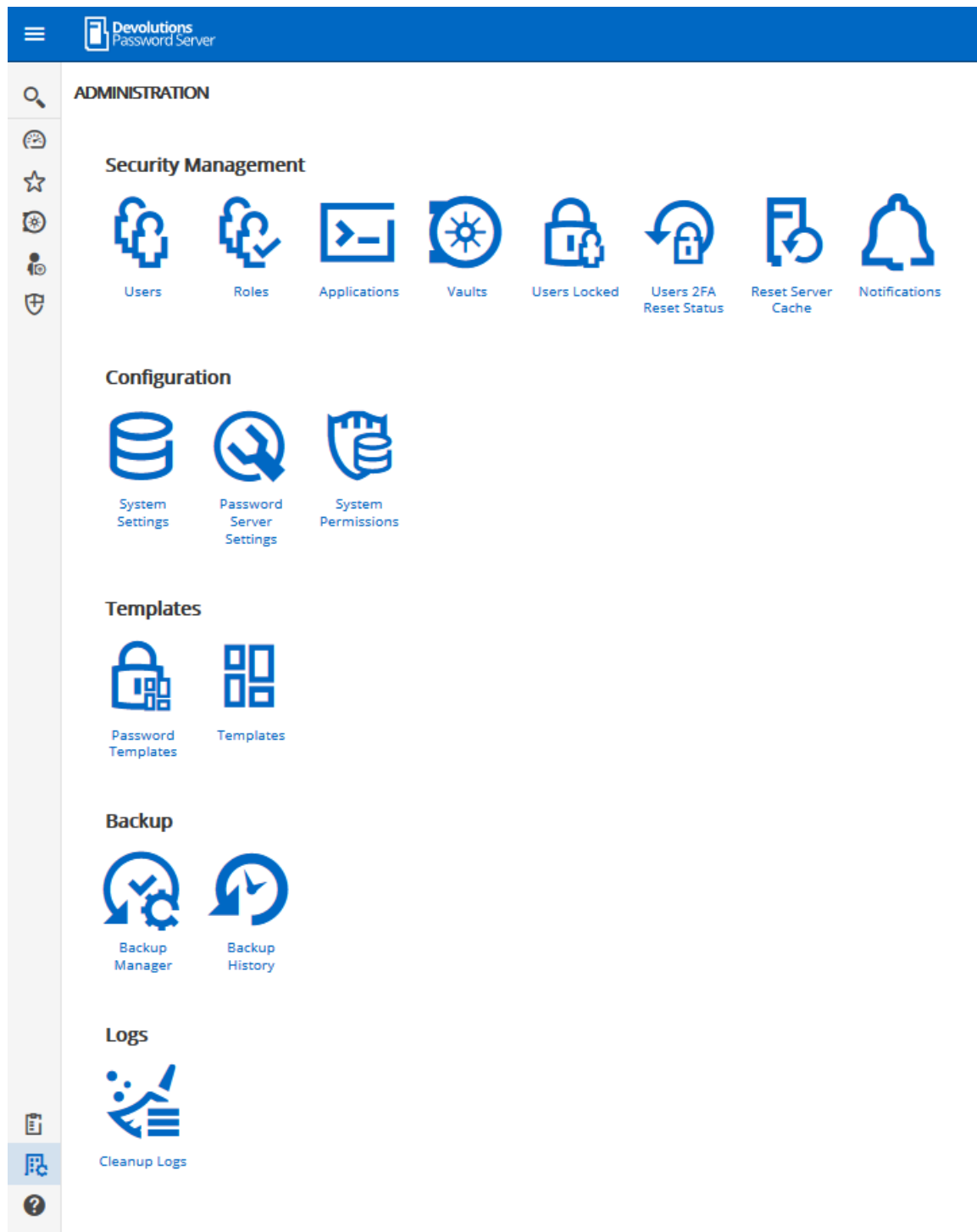
The Diagnostic report contains information such as the Devolutions Server and database version, the number of entries, the size of the data, etc. This report could be useful for troubleshooting or simply as an indication of your Devolutions Server content.

Reports - Diagnostic

5.5 Administration

DESCRIPTION

The **Administration** section is only available for administrators. Here you can find the various necessities to probably manage and customize your settings, ranging from security to the Backup system.

*Administration*









5.5.1 Security Management

5.5.1.1 Users

DESCRIPTION




Users is where you can create, import and manage users. To access the user management, navigate to **Administration – Users**. Click on a user to configure specific settings and permissions.

SETTINGS





ADMINISTRATION > USERS								
	Username	Full name	Authentication Type	User Type	Is enabled	Reset 2FA requested	Last Login	Last Login
	victor@windja	Victor Hedm...	Domain	User	✓	✗		
	sa		Database	Administrator	✓	✗		
	bill@windjamr	Bill Preston	Domain	User	✓	✗	1/28/2019 1...	a day ago
	ellen@windjar	Ellen Ross	Domain	User	✓	✗	1/29/2019 1...	3 hours ago
	jeff@windjamr	Jeff Smith	Domain	User	✓	✗	8/3/2018 11:...	6 months ago
	allan@windjar	Allan Brewer	Domain	User	✓	✗	7/25/2018 0...	6 months ago
	burton.guido@	Burton Guido	Domain	User	✓	✗		
	david@windja	David1 Hervi...	Domain	Administrator	✓	✗	1/29/2019 1...	an hour ago

Administration - Users

GLOBAL OPTIONS

Options	DESCRIPTION
	Add a user.
	Import users from LDAP.
	Refresh users list.

USER OPTIONS

Options	DESCRIPTION
	See user activity report.
	Change password.
	Edit user settings.
	Delete user.

5.5.1.1.1 General

DESCRIPTION

Edit user

GENERAL

INFORMATION

TWO FACTOR

ROLES

APPLICATIONS

VAULTS

SETTINGS

EMAIL NOTIFICATIONS

GENERAL

Authentication type

Office 365/Azure AD

User

ellen@downhillpro.xyz

User type

User

User license type

Default

☒ Enabled

☐ Must change password at next logon

INFORMATION

First name

Ellen

Last name

Ross

Email

ellen@windjammer.loc

UPDATE

CANCEL

Edit Users - General

OPTION	DESCRIPTION
Authentication type	<p>Select the user's authentication type:</p> <ul style="list-style-type: none">• Custom (Devolutions): create a user in Devolutions Server without creating an SQL login.• Domain : authenticate using the Active Directory user account.• Database (SQL Server): authenticate using the SQL login from your SQL Server.
User (required)	<p>Enter the user login name.</p>
User type	<p>Choose the user type:</p> <ul style="list-style-type: none">• Administrator: grant full administrative rights to the user.• Read only user: grant only the View access to the user.• Restricted user: select which rights to grant to the user.• User: grant all basic rights to the user (Add, Edit, Delete).
User license type	<p>Select the type of the license that the user has:</p> <ul style="list-style-type: none">• Default: Connection Management.• Connection Management: for users who open remote connections.• Password Management: for users who only use Devolutions Server as a password manager.
Enabled	<p>Check to activate the user.</p>
Must change password at next	<p>Check to force the user to change the password next time they log on.</p>

OPTION	DESCRIPTION
logon	
First name	Enter the user's first name.
Last name	Enter the user's last name.
Email (required)	Enter the user's email address.

5.5.1.1.2 Information

DESCRIPTION

The **Information** section is for optional information.

The screenshot shows the 'Edit user' dialog box with the 'INFORMATION' tab selected. The left sidebar contains a list of tabs: GENERAL, INFORMATION (highlighted), TWO FACTOR, ROLES, APPLICATIONS, VAULTS, SETTINGS, and EMAIL NOTIFICATIONS. The main area is divided into sections: INFORMATION, ADDRESS, and PHONE. The INFORMATION section includes fields for Company (with a required asterisk), Job title, Department, and Gravatar email (pre-filled with 'ellen@windjammer.loc'). The ADDRESS section includes fields for Address, State, and a Country dropdown menu (pre-selected with 'Select Country'). The PHONE section includes fields for Phone, Work, Mobile, and Fax. At the bottom right, there are 'UPDATE' and 'CANCEL' buttons.

Edit user	
GENERAL	INFORMATION
INFORMATION	
TWO FACTOR	
ROLES	
APPLICATIONS	
VAULTS	
SETTINGS	
EMAIL NOTIFICATIONS	

INFORMATION

Company *

Job title

Department

Gravatar email

ADDRESS

Address

State

Country

Select Country

PHONE

Phone

Work

Mobile

Fax

UPDATE CANCEL

Edit User - Information

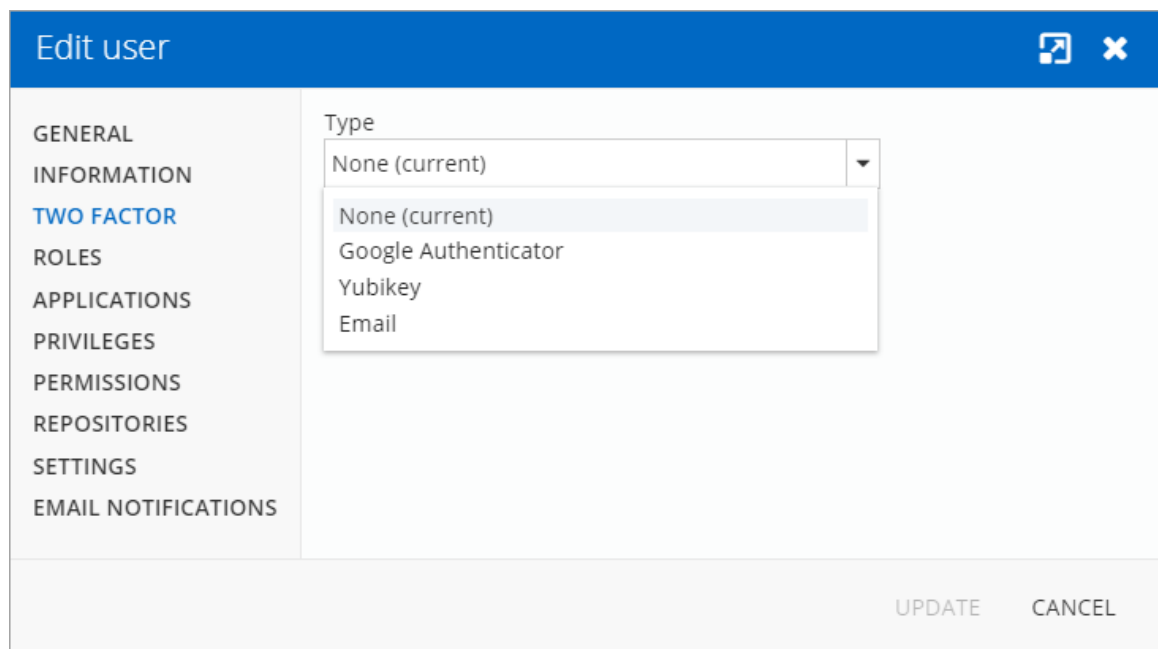
5.5.1.1.3 Two Factor

DESCRIPTION

If you set two-factor authentication as [optional per user in Password Server Settings](#), you then need to configure which 2FA method to use.

SETTINGS

1. Select the users 2FA **Type** from the list.



The screenshot shows a web interface window titled "Edit user". On the left is a sidebar with a list of tabs: GENERAL, INFORMATION, TWO FACTOR (highlighted in blue), ROLES, APPLICATIONS, PRIVILEGES, PERMISSIONS, REPOSITORIES, SETTINGS, and EMAIL NOTIFICATIONS. The main area of the window shows the "Type" dropdown menu for two-factor authentication. The dropdown is open, displaying the following options: "None (current)" (which is highlighted), "Google Authenticator", "Yubikey", and "Email". At the bottom right of the window, there are two buttons: "UPDATE" and "CANCEL".

Edit User - Two Factor

2. Choose if you **(a)** want the user to configure the 2FA next time they log in or **(b)** complete the set up now.

Edit user

GENERAL

INFORMATION

TWO FACTOR

ROLES

APPLICATIONS

PRIVILEGES

PERMISSIONS

REPOSITORIES

SETTINGS


EMAIL NOTIFICATIONS

Type

Google Authenticator


☐ Configure later by user

GoogleAuthenticator



Setup

1. Scan this QR code with your mobile app or use the key and account name below to setup your account.



Key

vTKtB69TTU

Account name

ellen@windjammer.loc

2. Submit the code given to you after scanning.

Validation code

Submit

UPDATE

CANCEL

Edit User - Two Factor

5.5.1.1.4 Roles

DESCRIPTION

Assign users to a **Role**.

Edit user

GENERAL
INFORMATION
TWO FACTOR
ROLES
APPLICATIONS
VAULTS
SETTINGS
EMAIL NOTIFICATIONS

i Only custom roles can be manually assigned.

X Unselect All ✓ Select All

Name ^	Description	Role Type ↕	Is member
WINDJAMMER\Vault ...	Password Vault Users	Active Directory	<input type="checkbox"/>
WINDJAMMER\Vault ...		Active Directory	<input type="checkbox"/>
WINDJAMMER\RDM ...	Service Desk Staff - I...	Active Directory	<input type="checkbox"/>
Show-IT Corp	Azure/Office365	Office365	<input checked="" type="checkbox"/>
WINDJAMMER\Vault ...	Groups from IT Depa...	Active Directory	<input type="checkbox"/>
Show-Corporate	Azure/Office365	Office365	<input checked="" type="checkbox"/>
WINDJAMMER\RDM ...	Full administrators	Active Directory	<input type="checkbox"/>
WINDJAMMER\Vault ...	CAL Non-IT Users	Active Directory	<input type="checkbox"/>
WINDJAMMER\HR		Active Directory	<input type="checkbox"/>
WINDJAMMER\Service...		Active Directory	<input type="checkbox"/>

UPDATE CANCEL

Edit User - Roles

OPTION	DESCRIPTION
Roles	Check the Is Member box to assign the role to the user. Consult Role Management topic for more information.

5.5.1.1.5 Applications

DESCRIPTION

Allow or deny the user access to different applications and companion tools:

Edit user

GENERAL
INFORMATION
TWO FACTOR
ROLES
APPLICATIONS
VAULTS
SETTINGS
EMAIL NOTIFICATIONS

ACCESS

Remote Desktop Manager
Allow

Devolutions Web Login
Allow

Devolutions Launcher
Allow

Web
Allow

Cli
Allow

UPDATE CANCEL

Edit User - Applications

OPTION	DESCRIPTION
Remote Desktop Manager	Allow user to access Devolutions Server through Remote Desktop Manager.
Devolutions Web Login	Allow user to auto fill username and passwords on websites with Devolutions Web Login.
Devolutions Launcher	Allow user to open remote connections with Devolutions Launcher.
Web	Allow user to use Devolutions Server web interface.
Cli	Allow user to use the Cli.

5.5.1.1.6 Vaults

DESCRIPTION

Select which **vaults** the user has access to.

For more information, please consult the [vaults](#) topic.

Name	Description	Allow
Downhill Pro	Customer since 2015	<input type="checkbox"/>
Telemark	Customer since 2017	<input type="checkbox"/>
Windjammer Corp	Password Vault for non-administrative per...	<input type="checkbox"/>
Windjammer Default	Default Repository - Shortcuts and commo...	<input type="checkbox"/>
Windjammer IT	For the IT departement exclusive use	<input type="checkbox"/>
Windjammer IT Vault	For IT personnel without the need for Con...	<input type="checkbox"/>

« 1 »

UPDATE CANCEL

Edit User - Vaults

5.5.1.1.7 Settings

DESCRIPTION

Offline mode

Read-only

UPDATE CANCEL

Edit User - Settings

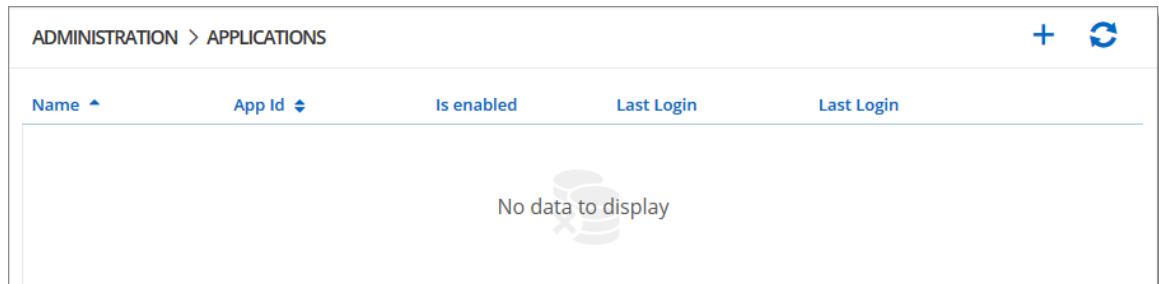
Allow the user to enable [Offline Mode](#) on the data source. The data source also needs to be configured to permit offline mode. There are 4 modes available:

OPTION	DESCRIPTION
Disabled	No offline cache allowed for the user.
Cache only	Allow to save a cache of the data source but not the offline mode.
Read-only	A read-only cache. The user will not be able to edit data in the data source. This mode is allowed for Advanced Data Sources only.
Read/Write	An advanced cache, with change synchronization. This mode is allowed for Advanced Data Sources only.

5.5.1.2 Applications

DESCRIPTION

The Applications section will allow to create an application key to communicate with Devolutions Server through the API SDK.



Administration - Applications

Application

GENERAL

ROLES

VAULTS

EMAIL NOTIFICATIONS

GENERAL

Copy the new Application Secret value. You won't be able to retrieve it once you leave this window.

Name

ApplicationKey

Application key

0648140d-e6df-4e2d-9a46-e0756183d793

Application Secret

KaGS6ww1Ph0OmIGEXZVWueyYh65e4Rtjh6e5W2uZsjcPaTQoj94b96VKxtFmHI82

☒ Enabled

Add

Cancel

Administration - Applications - New Application

GENERAL	DESCRIPTION
Name	Display name of the Application key.
Application key	Application key to be use in the application to communicate with Devolutions Server instance.
Application Secret	Secret key to be use in combination with the Application key. Available only on Application key creation.
Enabled	Activate the Application key.

5.5.1.3 Vaults

DESCRIPTION

The **Vaults** management allows to create and manage **Vaults**. To access the **Vaults** management, navigate to **Administration – Vaults**.

Name	Description	Actions
Downhill Pro	Customer since 2015	[Edit] [Add Users] [Remove Users] [Delete]
Telemark	Customer since 2017	[Edit] [Add Users] [Remove Users] [Delete]
Windjammer Corp	Password Vault for non-administrative personnel	[Edit] [Add Users] [Remove Users] [Delete]
Windjammer Default	Default Repository - Shortcuts and common tools	[Edit] [Add Users] [Remove Users] [Delete]
Windjammer IT	For the IT department exclusive use	[Edit] [Add Users] [Remove Users] [Delete]
Windjammer IT Vault	For IT personnel without the need for Connection Management	[Edit] [Add Users] [Remove Users] [Delete]

Administration - Vaults

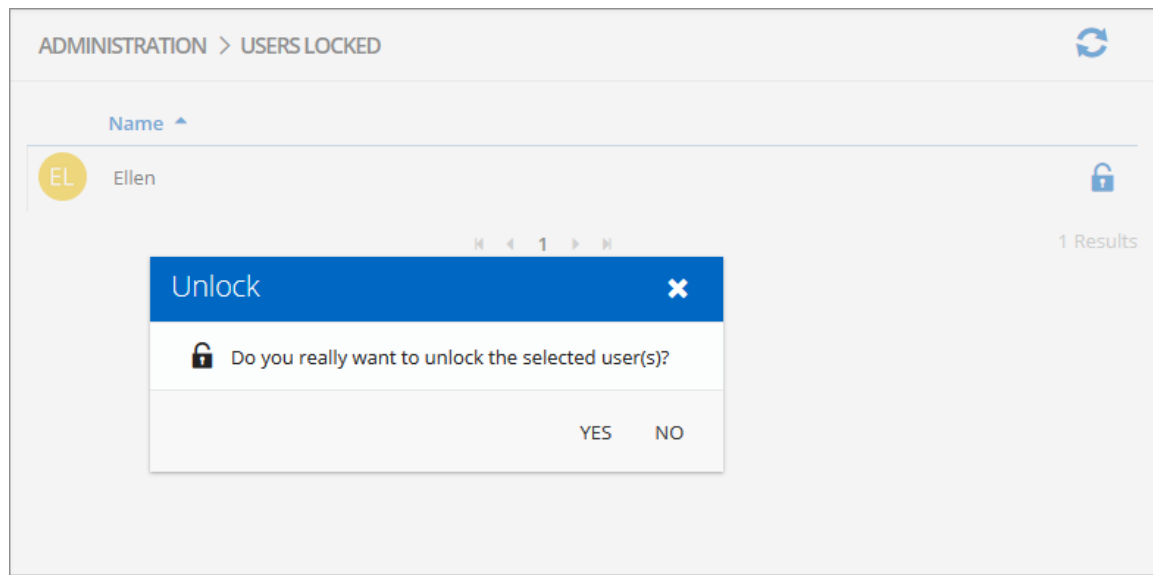
5.5.1.4 Users Locked

DESCRIPTION

The **Users Locked** allows to manage user accounts that has been locked after too many failed log in attempts. To access the **Users Locked** list, navigate to **Administration – Users Locked**.

Name	Status
EL Ellen	[Locked]

Administration - Users Locked

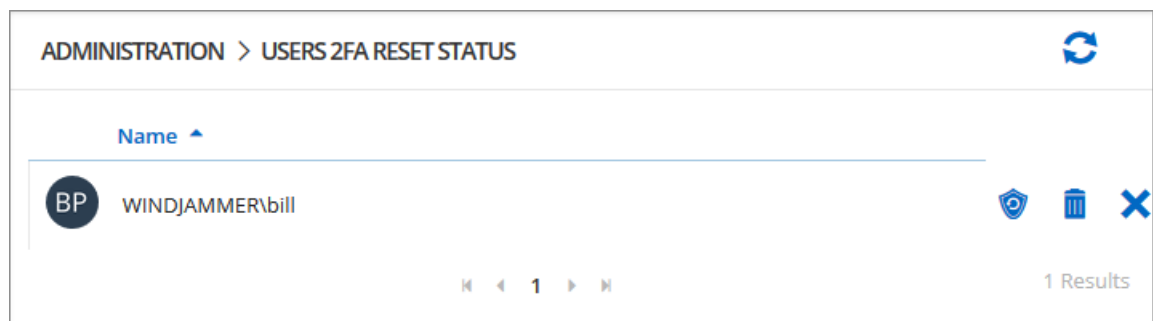


Unlock user account

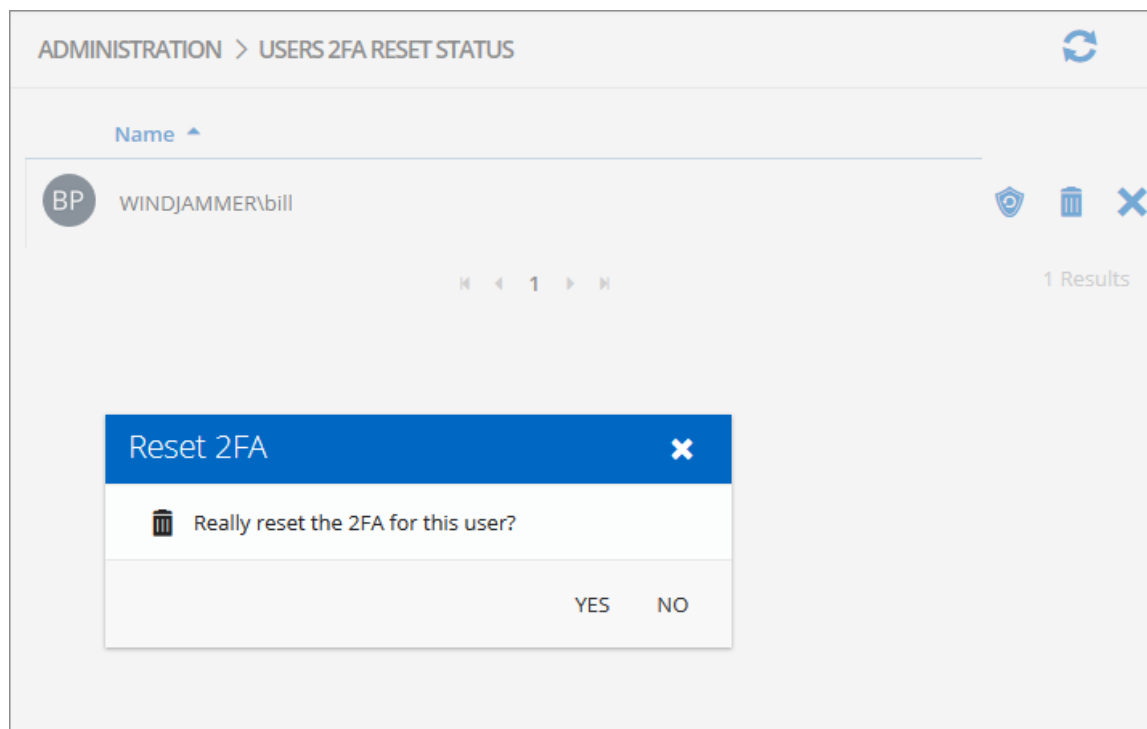
5.5.1.5 Users 2FA Status

DESCRIPTION

The **Users 2FA Status** section displays user accounts that have requested a 2FA reset. To access the list of users that ask for a 2FA reset, navigate to **Administration – Users 2FA Status**.



Administration - Users 2FA Reset Status

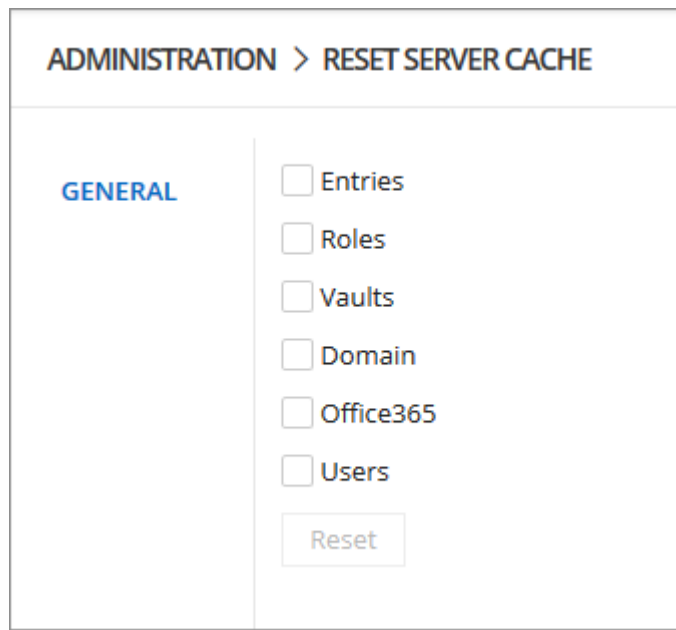


User 2FA Reset operation

5.5.1.6 Reset Server Cache

DESCRIPTION

Reset the **Server Cache** for specific elements.



ADMINISTRATION > RESET SERVER CACHE

GENERAL

- ☐ Entries
- ☐ Roles
- ☐ Vaults
- ☐ Domain
- ☐ Office365
- ☐ Users

Reset

Administration - Reset Server Cache

OPTION	DESCRIPTION
Entries Roles Vaults Users	When selecting one of those options, when resetting the cache, it will pull back all the information from the database and put the information in the server's memory cache.
Domain Office365	When resetting the Domain or the Office365 cache, it will wipe out the information saved in the database and will reload all the users and groups memberships pulled from Active Directory or from Azure AD.

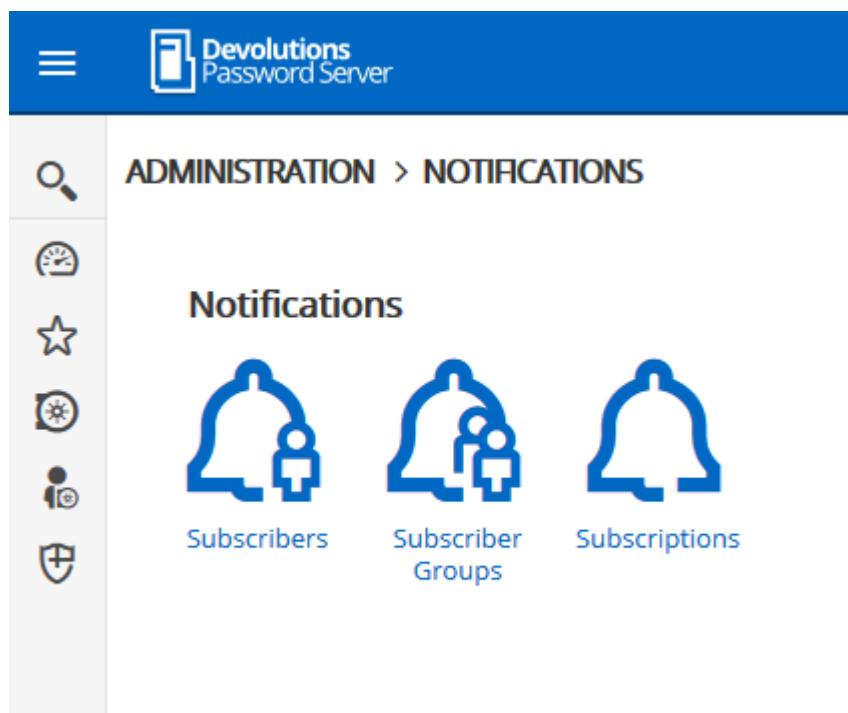
5.5.1.7 Notifications

DESCRIPTION



The [Email](#) and the [Scheduler](#) features must be enabled and properly configured to get the Notifications working.

With Devolutions Password Server, it is possible to get email notifications based on user activities with the Notification features.



Notifications

To get the Notification working, at least a [Subscriber](#) and a [Subscription](#) need to be created. It is also possible to regroup Subscribers in [Subscriber Groups](#) to send notifications to a group of subscribers.

The following sample represents a notification email that has been received for an entry creation.



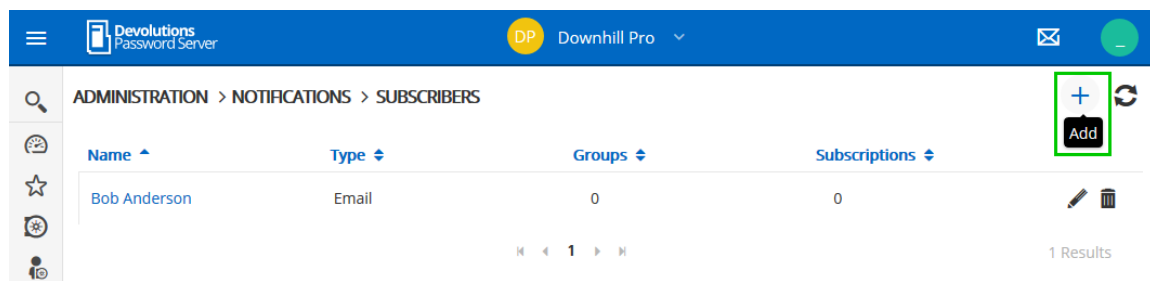
Email notification sample

5.5.1.7.1 Subscribers

DESCRIPTION

At least, one subscriber must exist to receive notifications about Devolutions Password Server activities.

To create a new Subscriber, click on the Add button.



Create a Subscriber

Fill in the information in the following fields.

The screenshot shows the 'Subscriber' form. It has a title bar with the word 'Subscriber' and a close button. The form contains the following fields:

- Name**: A text input field containing 'Bob Anderson'.
- Type**: A dropdown menu with 'Email' selected.
- EMAIL**: A section header.
- Email Address**: A text input field containing 'bob@windjammer.co'.
- Recipient Name**: A text input field containing 'Bob Anderson'.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom right.


Email Subscriber properties

Subscriber

Name •

Type •

LOG TO SYSLOG SERVER

☐ Use default 

Host Name: •

Port: •

Protocol: •

Save **Cancel**

Syslog Server Subscriber properties

OPTION	DESCRIPTION
Name	Display of the Subscriber.
Type	<ul style="list-style-type: none">• Email : The notification will be sent to an email address.<ul style="list-style-type: none">○ Email Address: Valid email address.○ Recipient name: Email recipient name.



OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Syslog : The notification will be sent to a syslog server.<ul style="list-style-type: none">○ Use default: Will use the Syslog server configuration set in Logging.○ Host name: Host name of the Syslog server.○ Port: Port of the syslog server.○ Protocol: Protocol (TCP or UDP) to communicate with the Syslog server.

5.5.1.7.2 Subscriber Groups

DESCRIPTION



The Subscriber Groups can be used to regroup [Subscribers](#) and allow to send [Subscriptions](#) to a group of people and/or syslog servers.



Subscriber Group





Name ●

SUBSCRIBERS

Bob Anderson

Kelly Slater

Syslog Server

+ Add Subscriber

Save

Cancel

Subscriber Group properties dialog

OPTION	DESCRIPTION
Name	Name of the Subscriber Group.
Subscribers	List of subscribers that are member of the subscriber group. users and Syslog subscribers can be added in a subscriber group.

5.5.1.7.3 Subscriptions

DESCRIPTION

The subscriptions are intended to send email according to activities on Devolutions Server. It could be activities on entries, user accounts, system settings, etc.

Subscription

Name •

Subscriber •

Select Subscriber

Subscription Category •

Entry

FILTERS

+ Add Filter

Save

Cancel

Subscription properties dialog

OPTION	DESCRIPTION
Name	Name of the Subscription.
Subscriber	One subscriber that will receive the notifications from the current subscription. A subscriber or a subscriber group can be selected.
Subscription Category	Category of the subscription. This can be one of the following possibilities. <ul style="list-style-type: none">• Entry• User Vault• Role• PAM Privileged Account

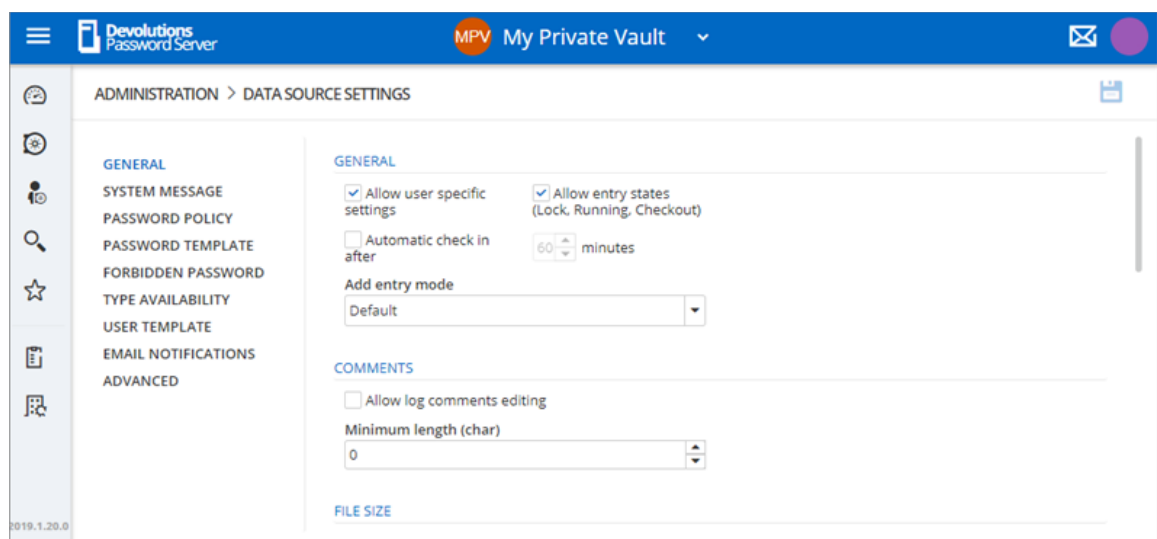
OPTION	DESCRIPTION
	<ul style="list-style-type: none"> • PAM Provider • PAM Checkout • PAM Folder • System Settings
Filters	The filters are tied to the subscription category and each of them has their own filters. You can add a filter with the Add Filter button. Be aware that the filters are cumulative.

5.5.2 Configuration

5.5.2.1 System Settings

DESCRIPTION

The System Settings allow the administrators control many global aspects of the Devolutions Server data source. Manage settings such as Password policy, Password Template, Type Availability, etc.



Administration - System Settings

5.5.2.1.1 General

DESCRIPTION

The General section of the System Settings allow the administrators to apply general policies for the whole data source.

The screenshot displays the 'Administration > System Settings' interface. On the left, a sidebar lists settings categories: GENERAL, SYSTEM MESSAGE, PASSWORD POLICY, PASSWORD TEMPLATE, FORBIDDEN PASSWORD, TYPE AVAILABILITY, USER TEMPLATE, EMAIL NOTIFICATIONS, and ADVANCED. The 'GENERAL' section is active, showing the following settings:

- GENERAL**
 - ☒ Allow user specific settings
 - ☐ Automatic check in after: 60 minutes
 - Add entry mode: Default (dropdown)
- COMMENTS**
 - ☐ Allow log comments editing
 - Minimum length (char): 0
- FILE SIZE**
 - Maximum file size (MB): 25

Administration - System Settings - General

GENERAL	DESCRIPTION
Allow user specific settings	Allow users to save User Specific Settings.
Allow entry states (Lock, Running, Checkout)	Allow entries to be locked when used or edited.
Automatic check in after	
Add entry mode	Select if users are prompted to choose a template when creating a new entry. Select between: <ul style="list-style-type: none"> • Default • Template list (include blank) • Template list only

GENERAL	DESCRIPTION
	<ul style="list-style-type: none">• No template selection

COMMENTS	DESCRIPTION
Allow log comments editing	Enable the log comment editing for all users.
Minimum length (char)	Minimum length in character for the comment.

FILE SIZE	DESCRIPTION
Maximum file size (MB)	Limit the size of attachments and document entries to avoid to over load the data source.

FAVORITES	DESCRIPTION
Allow favorites	Allows to flag entries as favorites.

Private Vault	DESCRIPTION
Allow Private Vault	Allow users to use the Private Vault .
Log Private Vault activities	Include the logs of the Private Vault for all users of the data source.
Allow credential repository in private	Allow credential repository for sessions in the Private Vault .

Private Vault	DESCRIPTION
Vault	

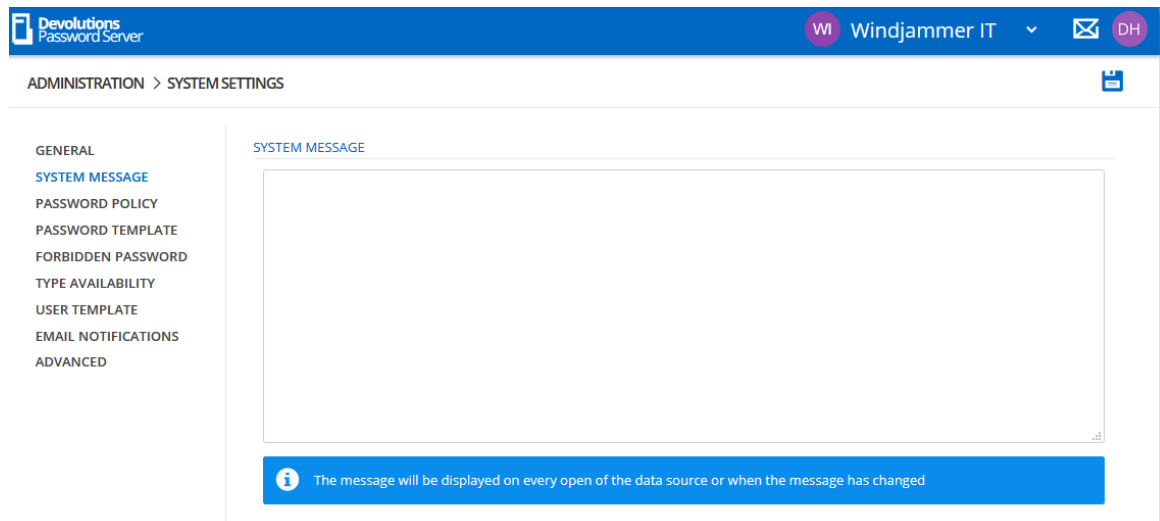
SECURITY	DESCRIPTION
Use legacy security	Enable the legacy security

SECURITY - TIME-BASED USAGE	DESCRIPTION
Time Zone	Select the time zone you are currently in.
Days	<p>Select which days the session is available for. Select between:</p> <ul style="list-style-type: none">• Any day: the session can be used any day of the week or week-end.• Week days: the session can be used only the week days.• Week ends: the session can be used only the week ends.• Custom: manually select each day the session is available for.
Time of day	<p>Select the hours which the session is limited to. Select between:</p> <ul style="list-style-type: none">• Any time: the session can be used at any hour.• Custom: manually select the time frame the session is available for.

5.5.2.1.2 System Message

DESCRIPTION

The **System Message** allows to set a message that will be displayed every time a user connects on the Devolutions Server data source no matter which method will be used (web interface, Remote Desktop Manager).

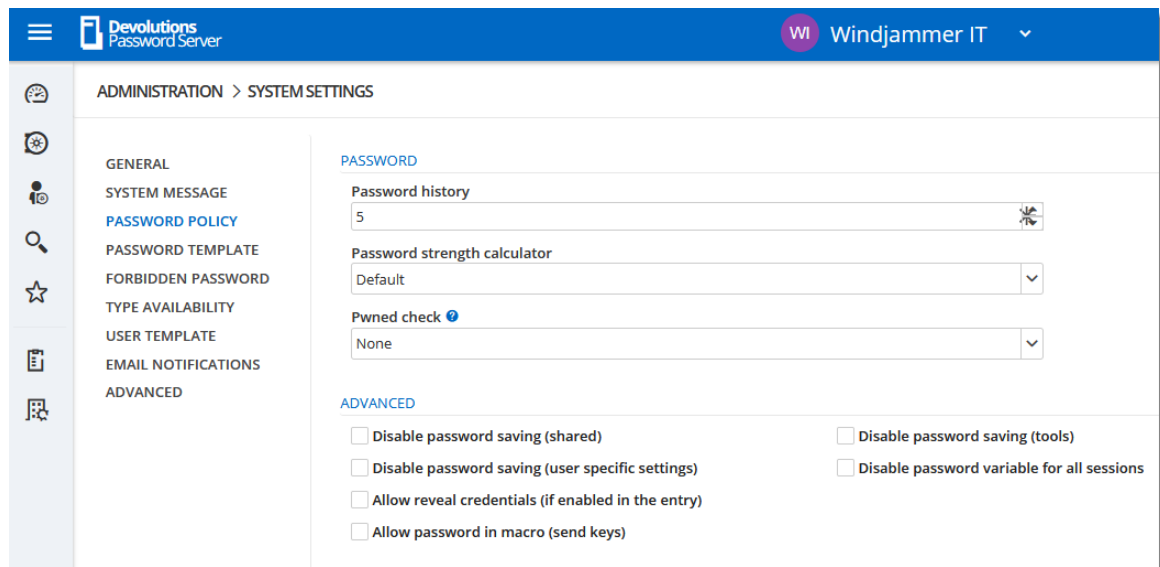


Administration - System Settings - System Message

5.5.2.1.3 Password Policy

DESCRIPTION

The **Password Policy** settings allow to set the minimal requirements for passwords that will be saved in the entries.



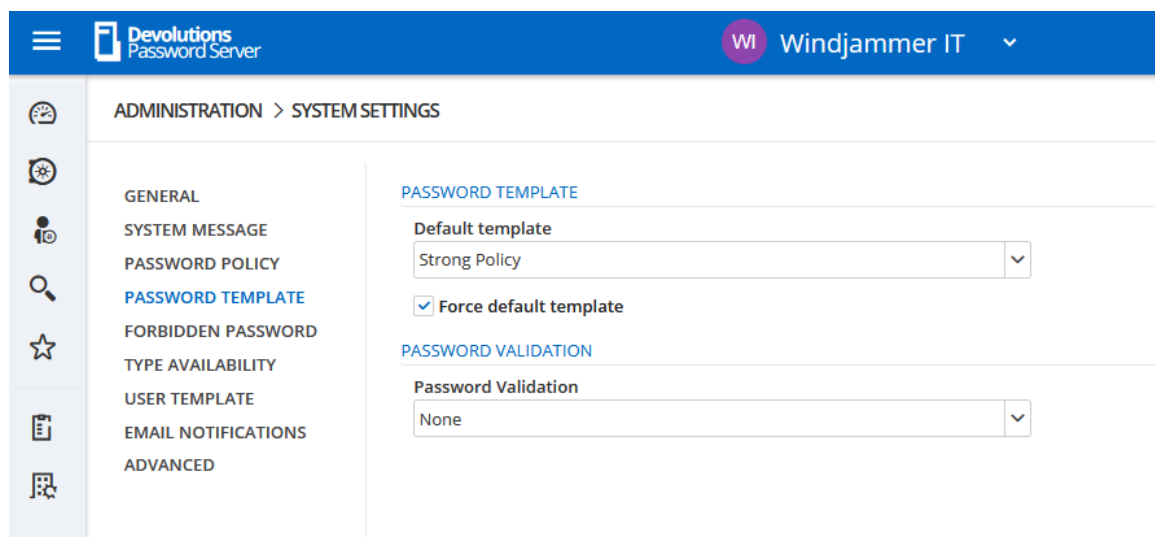
Administration - System Settings - Password Policy

PASSWORD	DESCRIPTION
Password History	Indicate the maximum saved password to keep in history.
Password strength calculator	Select the tool to use to analyze the password strength.
Pwned check	Verify if the used passwords have already been exposed to data breaches.
ADVANCED	DESCRIPTION
Disable password saving (shared)	Prevent users from saving passwords in entries.
Disable password saving (user specific settings)	Prevent users from saving passwords in the User Specific Settings.
Allow reveal credentials (if	Shows the credentials if the box "Allow show credentials (everybody)" is check inside the entry.

ADVANCED	DESCRIPTION
enabled in the entry)	
Allow password in macro (send keys)	Renders the \$MACRO_PASSWORD\$ variable useless for this data source.
Disable password saving (tools)	Prevent users from saving passwords in the Tools tab of a session.
Disable password variable for all sessions	Renders the \$PASSWORD\$ variable unusable for this data source.

5.5.2.1.4 Password Template

DESCRIPTION



Administration - System Settings - Password Template

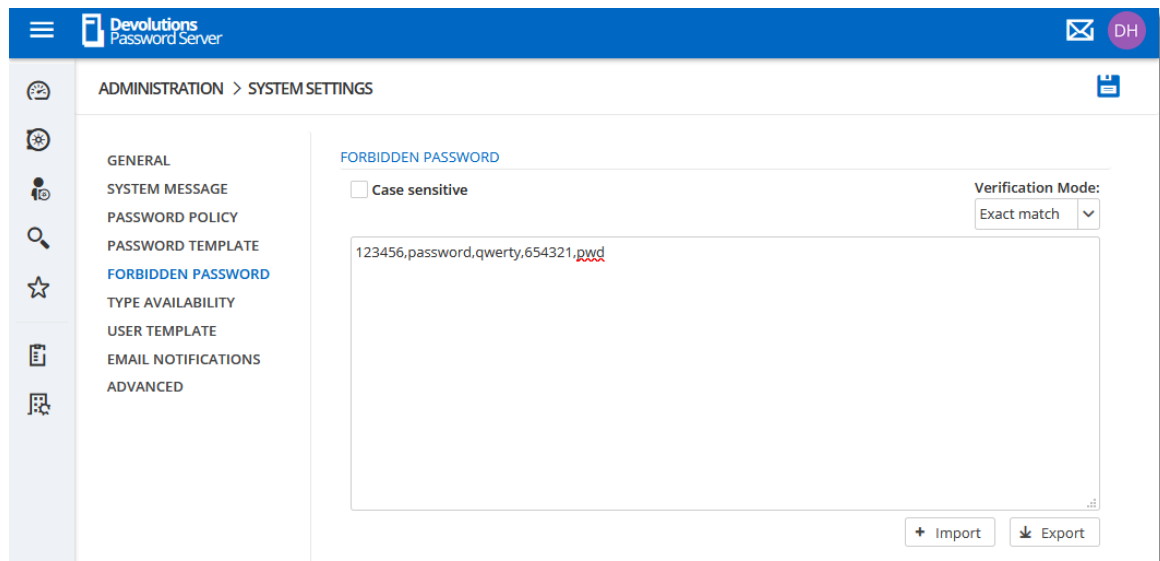
SETTINGS

PASSWORD TEMPLATES	DESCRIPTION
Password Validation	Select a password template to use. Consult the Password Template page for more information.
Force default template	Enforce the default template.
Password Template	<ul style="list-style-type: none">• None : No password templates will be used on password creation.• Required : On password creation, the user will get a warning that the password doesn't meet the Password Template rules. The user cannot save the password.• Warning : On password creation the user will get a warning that the password doesn't meet the Password Template rules. The user can save the password.

5.5.2.1.5 Forbidden Password

DESCRIPTION

Forbidden Passwords allow to create a list of blacklisted passwords to forbid usage in the application. Once set in this list, the password cannot be used anymore in the Devolutions Server data source.



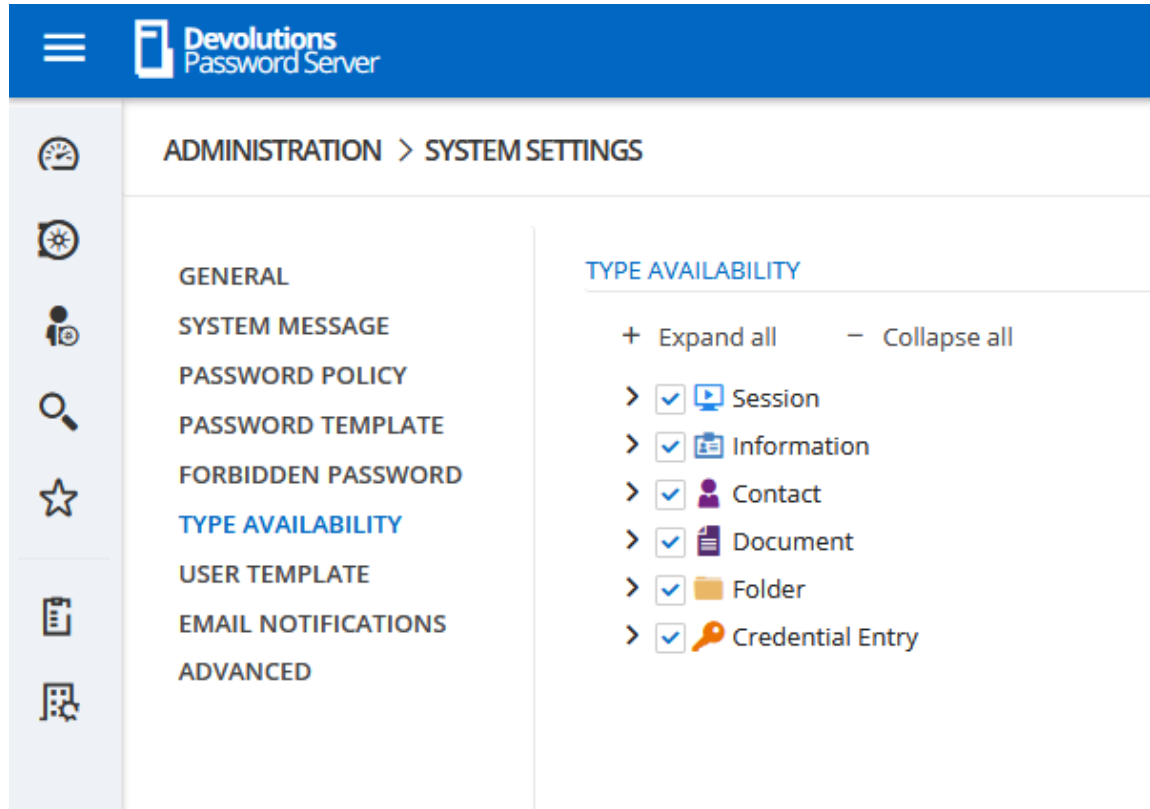
Administration - System Settings - Forbidden Password

OPTION	DESCRIPTION
Case sensitive	Make the verification mode case sensitive.
Verification mode	<p>Select the verification mode between:</p> <p>Contains: the password will be forbidden if it contains a word in the blacklist.</p> <p>Exact match: the password will be forbidden if it matches a word in the blacklist.</p>
Import	Import a list from your computer (*.pwd or .txt).
Export	Export your forbidden password list. By default the list will be exported in a password file format (.pwd).

5.5.2.1.6 Type Availability

DESCRIPTION

This section will allow to control the availability of the session, information, contact, document, folder, credential entry in Devolutions Server data source. Each section contains different entry types you can choose to be available.

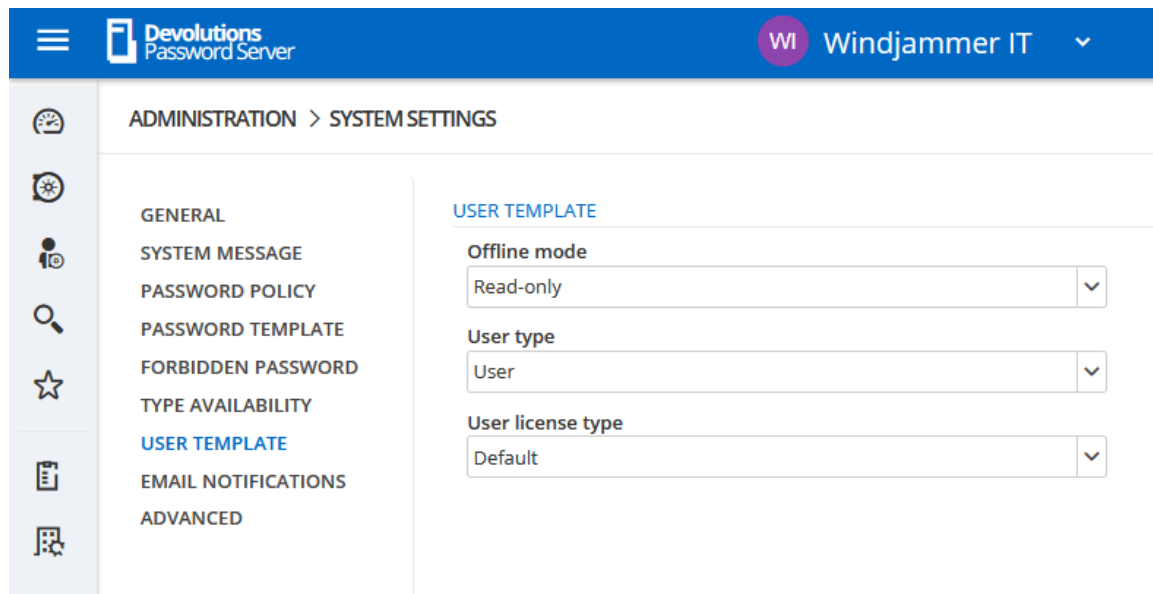


System Settings - Type Availability

5.5.2.1.7 User Template

DESCRIPTION

This section will set the user template for the [Automatic User Creation](#) feature.

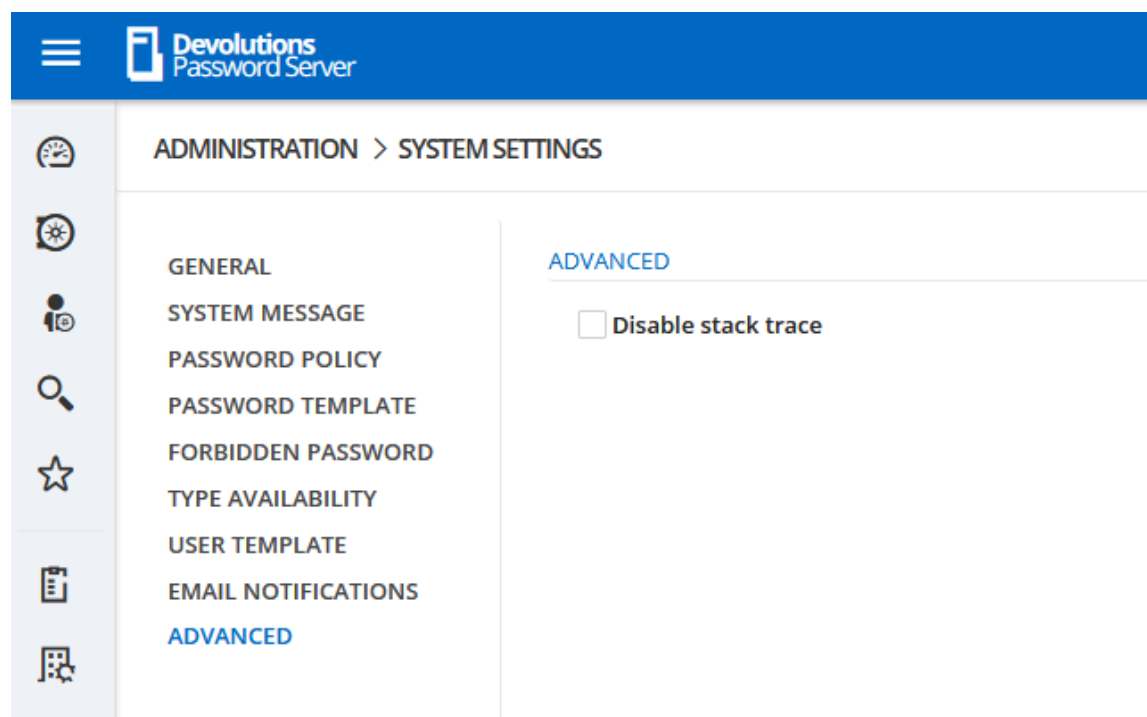


System Settings - User Template

OPTION	DESCRIPTION
Offline mode	<p>This option will only affect Remote Desktop Manager application.</p> <p>The possible values are :</p> <ul style="list-style-type: none"> • Disabled • Read only • Read/write
User type	<p>The possible values are :</p> <ul style="list-style-type: none"> • Administrator • User • Read only user
User license type	<p>Select if users are prompted to choose a template when creating a new entry. Select between:</p> <ul style="list-style-type: none"> • Default • Connection Management • Password Management

5.5.2.1.8 Advanced

DESCRIPTION

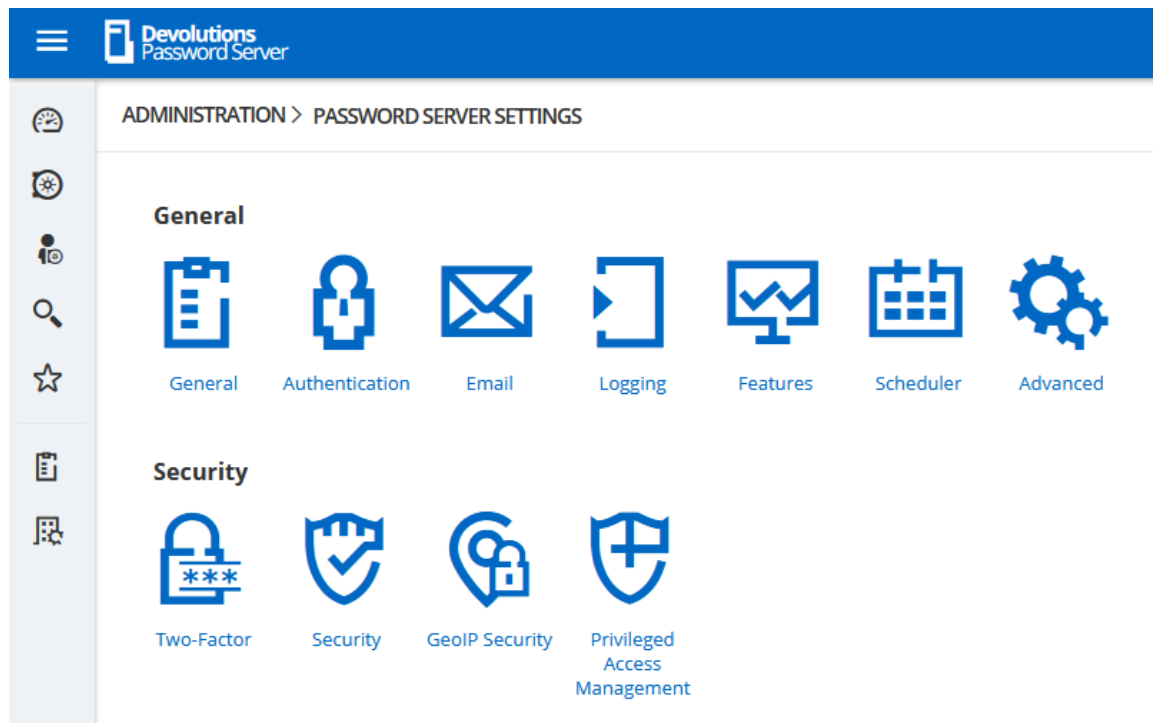


Administration - System Settings - Advanced

5.5.2.2 Password Server Settings

DESCRIPTION

The **Password Server Settings** page allows to manage the Devolutions Server configuration remotely.




Administration - Password Server Settings

5.5.2.2.1 General

5.5.2.2.1.1 General

DESCRIPTION

The **General** section allows the Administrator to modify the name or the description of the Devolutions Server instance.

ADMINISTRATION > PASSWORD SERVER SETTINGS > GENERAL 

GENERAL

Name

Description

DNS Name

SERIAL

Server

User limit: Unlimited users

Edition: Platinum

Expiration:

User CAL

User limit: 1 users

Launcher CAL

User limit: 1 users

Administration - Password Server Settings - General

SETTINGS

GENERAL

OPTION	DESCRIPTION
Name	Enter the name for your server, it will be displayed in the Content area.
Description	Enter a short description or additional information.

OPTION	DESCRIPTION
DNS Name	Name of the DNS server.

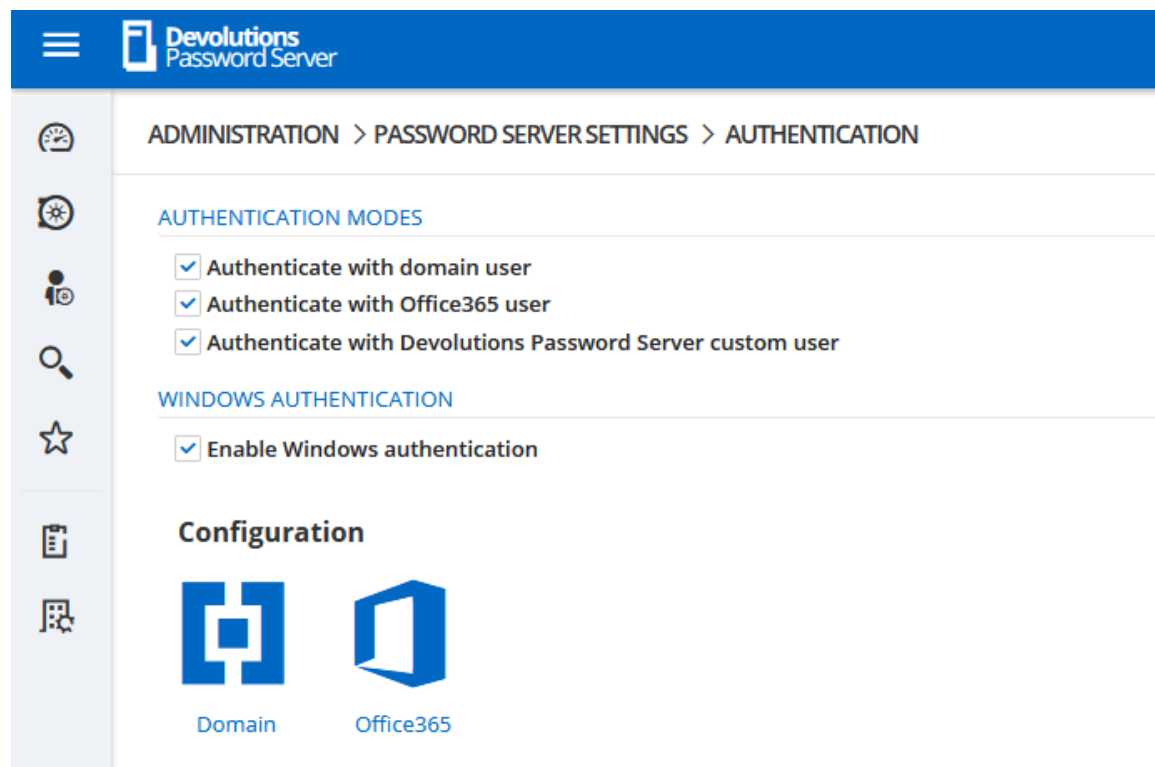
SERIAL

OPTION	DESCRIPTION
Serial	Insert your serial registration number.
User CAL	Insert your Client Access License keys.
Launcher CAL	Insert your Launcher License keys.

5.5.2.2.1.2 Authentication

DESCRIPTION

The **Authentication** section allows the Administrator to select which authentication types will be used



Administration - Password Server Settings - Authentication

SETTINGS

AUTHENTICATION MODES

OPTION	DESCRIPTION
Authenticate with domain user	The domain is used to authenticate the user.
Authenticate with Office365 user	AzureAD is used to authenticate the user.
Authenticate with Devolutions Server custom user	The Devolutions Server is used to authenticate the user. You must create the initial user through the console.

OPTION	DESCRIPTION
Enable Windows authentication	The application will use the current Windows authenticated user to authenticate to the Devolutions Server instance.

CONFIGURATION

OPTION	DESCRIPTION
Domain	Configure the Domain type.
Office365	Configure the Office365 type.

DESCRIPTION

The domain is used to authenticate the user. This is the most secure, flexible and easiest to manage. No need to sync users between the domain and Devolutions Server. On first use of the Devolutions Server data source, the user will be created and be given access rights according to their role in the organization as defined on the domain. You simply need to grant appropriate permissions to your roles in Devolutions Server. Upon authentication we will validate the AD groups to which the user belongs and for any that have a corresponding role we will grant the permissions to the user.

ADMINISTRATION > PASSWORD SERVER SETTINGS > AUTHENTICATION > DOMAIN

DOMAIN AUTHENTICATION

Domain



Container

Administration credentials

[Change](#)☐ Allow logins using email address

LDAPS

☐ Enable LDAPS

Port

☒ Default☐ Custom

MULTI DOMAIN (DISABLED)

☐ Multi domain

Trusted domains

[Change](#)

AUTOMATIC USER CREATION

☐ Auto create domain users in database☒ Create read-only user

Default Vault



Only from this AD group

[Change](#)

Username Format



DOMAIN USERS AND ROLES CACHE

☒ Enable domain cache feature

Update users and groups data every:

Hours

Minutes

Authentication - Configure Domain

SETTINGS

DOMAIN AUTHENTICATION

OPTION	DESCRIPTION
Domain	Specify the remote computer domain name.
Container	Specify the Active Directory Organizational Unit (OU) or Group to restrict the search in a specific area in the Active Directory structure. The format must be the distinguished name (CN=Users,DC=windjammer,DC=loc).
Administration credentials	Add the credentials of a domain or service account to access the Active Directory forest and obtain user account information through LDAP queries. This is needed when the server hosting the instance is not located on the domain. This account needs to be a member of the Account Operators AD group in order to have enough permissions to retrieve user account information and group memberships.
Allow logins using email address	Allow users to use their email address to connect to the Devolutions Server instance. The email address field must be filled in the User Management.

LDAPS

OPTION	DESCRIPTION
Enable LDAPS	Enable the LDAP over SSL communication.
Port	Default: LDAPS default communication port.

OPTION	DESCRIPTION
	Custom: Set a specific port value.

MULTI DOMAIN (DISABLED)



The Multi Domain feature requires the Devolutions Server Platinum Edition license. Currently, it is only working with trusted domains that belong to the same AD Forest.

OPTION	DESCRIPTION
Multi domain	Enable the Multi domain feature.
Trusted domains	Add your trusted domains.

AUTOMATIC USER CREATION

OPTION	DESCRIPTION
Auto create domain users in database	Automatically create the domain user account in the the database on the first login attempt.
Create read-only user	When this option is enabled, the user account will be created as a Read only user type account.
Default Vault	Will give access to that Vault to the user.
Only from this AD group	Will create automatically the user only if he is a member of this AD group.

OPTION	DESCRIPTION
Username Format	<p>Select the username format that will be created in the database.</p> <ul style="list-style-type: none">• UPN : The user will be created using the UPN format ex: bill@windjammer.loc.• NetBios : The user will be created using the NetBios format ex: WINDJAMMER\bill.• Username : The user will be created using the SAM account name.

DOMAIN USERS AND ROLES CACHE

OPTION	DESCRIPTION
Enable domain cache feature	Activate the domain cache feature.
Update users and groups data every:	Set the hours and minutes period that the Domain Users and Roles Cache will be refreshed. When enable, the default value is set to 30 minutes.

DESCRIPTION



Microsoft Azure Active Directory subscription is required to configure Office365 authentication in Devolutions Server. You need to create three new app registrations in Microsoft Azure Active Directory before completing the authentication settings. For more information about the app registrations, see [Azure portal configuration guide for Office 365 authentication](#).

The **Office365** tab allows Devolutions Server to authenticate users using **Office365 authentication**. All fields are mandatory.

ADMINISTRATION > PASSWORD SERVER SETTINGS > AUTHENTICATION > OFFICE365

OFFICE365 PARAMETERS

Tenant ID
4c5a5ec1-9ac5-4612-9b4c-6bed178bb65a

Native application (RDM)
Client ID
dd5497f9-6cb7-42ef-97c0-ff343de677ea
Resource ID
00000002-0000-0000-c000-000000000000
Redirect URI
http://vwindsrv-dvls4/newshowcase

Web application
Client ID
214af327-0696-4278-9fc0-da90bacb9e90

Users and Roles Cache
Client ID
b955972a-1384-4b72-9f9e-38b6e57269d6 *
Redirect URI
http://vwindsrv-dvls4/newshowcase *
Secret key
*

AUTOMATIC USER CREATION
☐ Auto create domain users in database
☐ Create read-only user
Default Vault
Windjammer Default

OFFICE365 USERS AND ROLES CACHE
Update users and groups data every:
0 Hours 30 minutes
Test Connection

Authentication - Configure Office365

SETTINGS

OFFICE365 PARAMETERS

OPTION	DESCRIPTION
Tenant ID	The TenantID is the Directory ID of the Azure Active Directory.

NATIVE APPLICATION (RDM)

OPTION	DESCRIPTION
Client ID	Application ID of the Azure AD application.
Resources ID	resourceAppid from the Manifest of the Azure AD application.
Redirect URI	Redirect URI from the Azure AD application.

WEB APPLICATION

OPTION	DESCRIPTION
Client ID	Application ID from the web app section of the Azure AD application.

USERS AND ROLES CACHE

OPTION	DESCRIPTION
Client ID	Application ID of the Azure AD application.
Redirect URI	Redirect URI from the Azure AD application.
Secret Key	Key from the Password generated in Settings - Keys of the Azure AD application.

AUTOMATIC USER CREATION

OPTION	DESCRIPTION
Auto create domain users in database	Automatically create the Office365 user account in the database on the first login attempt.
Create read-only user	Set the user account as a read-only account.
Default Vault	Will give access to that Vault to the user.


OFFICE365 USERS AND ROLES CACHE

OPTION	DESCRIPTION
Update users and groups data every:	Set the hours and minutes period that the Office365 Users and Roles Cache will be refreshed. Default value is set to 30 minutes.

5.5.2.2.1.3 Email

DESCRIPTION

Emails are sent by our Notification engine and by some of our 2 factor authentication providers.

ADMINISTRATION > PASSWORD SERVER SETTINGS > GENERAL 

GENERAL

Name

Devolutions Password Server

Description

Devolutions inc.

DNS Name

SERIAL

Server

User limit: Unlimited users

Edition: Platinum

Expiration:

User CAL

User limit: 1 users

Launcher CAL

User limit: 1 users

Administration - Password Server Settings - Email

SETTINGS

GENERAL

OPTION	DESCRIPTION
Email enabled	Enable the Email feature.

SMTP CONFIGURATION

OPTION	DESCRIPTION
Host	Name or IP address of the SMTP server.
Port	Set the SMTP server port.
SSL enabled	Specifies whether to use Secure Sockets Layer (SSL) to encrypt the connection. Please see Note 1 for important information.
Username	Enter your username to connect to your SMTP server.
Password	Enter your password to connect to your SMTP server.
Send email as	Sender email address.
Email administrator	Recipient email address that will receive the errors.
Test Email	Test your email settings.

NOTE 1


Devolutions Server only supports the **SMTP Service Extension for Secure SMTP over Transport Layer Security** as defined in RFC 3207. In this mode, the SMTP session begins on an unencrypted channel, then a **STARTTLS** command is issued by the client to the server to switch to secure communication using SSL.

An alternate connection method is where an SSL session is established up front before any protocol commands are sent. This connection method is sometimes called **SMTP/SSL**, **SMTP over SSL** or **SMTPS** and by default uses port 465. This alternate connection method using SSL is not currently supported.

5.5.2.2.1.4 Logging

DESCRIPTION

The **Logging** section allows the administrator to configure the logging features.

ADMINISTRATION > PASSWORD SERVER SETTINGS > LOGGING 

GENERAL

☒ Log debug information

Language
English ▼

Scheduler log path

SYSLOG SERVER

☐ Log to Syslog server

Host

Port

Protocol
TCP ▼

WINDOWS EVENT LOG

☐ Event Log

SLACK INTEGRATION

☐ Post activity logs to Slack

Bot OAuth access token

Slack channel name

Administration - Password Server Settings - Logging

SETTINGS

GENERAL

OPTION	DESCRIPTION
Log debug information	Enable the Devolutions Server instance logs. When enabled, this will raise the debug level and provide more log entries.
Language	Choose the language of the logs.
Scheduler log path	Set the destination path of the log file.

SYSLOG SERVER

OPTION	DESCRIPTION
Log to Syslog server	Send the logs to a Syslog Server.
Host	Enter your Syslog Server host to connect.
Port	Enter your Syslog Server port to connect.
Protocol	Select your preferred Protocol mode between: <ul style="list-style-type: none">• TCP• UDP

WINDOWS EVENT LOG

OPTION	DESCRIPTION
Event Log	Send the logs to Windows Event Log.


SLACK INTEGRATION

OPTION	DESCRIPTION
Post activity logs to Slack	Post the logs in a Slack channel.
Bot OAuth access token	Slack authentication access token.
Slack channel name	Name of the Slack channel where the logs will be posted.

5.5.2.2.1.5 Features

DESCRIPTION

The **Features** section allows the administrator to configure the web interface features.

ADMINISTRATION > PASSWORD SERVER SETTINGS > FEATURES 

☒ Allow browser extensions (Devolutions Web Login)

☐ Allow Devolutions Proxy

☐ Allow Web API help page

Administration - Password Server Settings - Features

SETTINGS

OPTION	DESCRIPTION
Allow browser extensions (Devolutions Web Login)	Allow to save credentials in the Devolutions Server instance with Devolutions Web Login.
Devolutions Proxy	Enable the Devolutions Proxy feature.
Allow Web API help page	


5.5.2.2.1.6 Scheduler

DESCRIPTION

The **Scheduler** is used to enable automated tasks in Devolutions Server. Some further configurations are needed to be done before enabling these options.



The [Email](#) settings must be configured in the Devolutions Server instance in order for notifications to be sent.

ADMINISTRATION > PASSWORD SERVER SETTINGS > SCHEDULER 

NOTIFICATION

☐ Allow notification subscription

Time Zone
(UTC-05:00) Eastern Time (US & Canada) ▼

Administration - Password Server Settings - Scheduler

NOTIFICATION

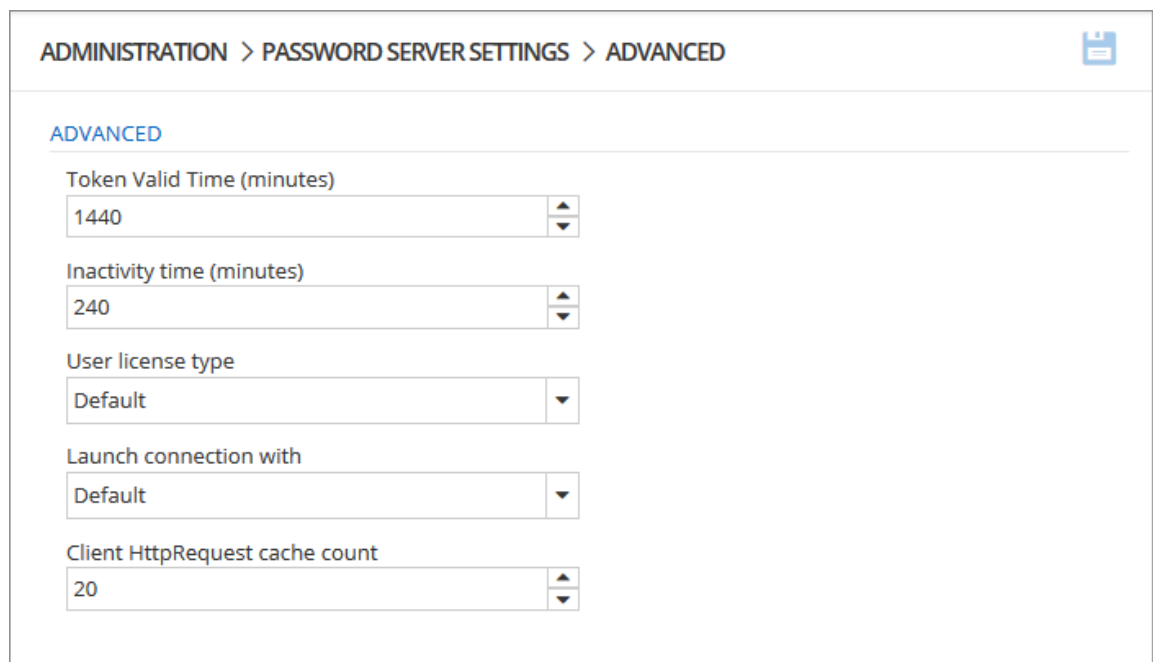
The **Notifications** settings are used to send email notifications to specific users. These notifications include any activities on sessions, roles, users, etc.

CATEGORY	DESCRIPTION
Allow notification subscription	Enable the notifications of the Devolutions Server instance.
Time Zone	Time zone used to display the time stamp in the notification email.

5.5.2.2.1.7 Advanced

DESCRIPTION

The **Advanced** section allows the administrator to configure the **Token Valid Time** parameter.



The screenshot shows the 'ADMINISTRATION > PASSWORD SERVER SETTINGS > ADVANCED' page. The 'ADVANCED' section is highlighted. It contains five settings:

- Token Valid Time (minutes)**: A numeric input field with the value 1440.
- Inactivity time (minutes)**: A numeric input field with the value 240.
- User license type**: A dropdown menu with 'Default' selected.
- Launch connection with**: A dropdown menu with 'Default' selected.
- Client HttpRequest cache count**: A numeric input field with the value 20.

Administration - Password Server Settings - Advanced

SETTINGS

FEATURES

CATEGORY	DESCRIPTION
Token Valid Time (minutes)	This the duration time of the token. At the expiration of the token, the user must again authenticate himself on the Devolutions Server instance. The maximal value is 10080 minutes which is 7 days.
Inactivity time (minutes)	Enter the delay for the user to be disconnected from the server if inactive. This value must be lower than the Toke Valid Time parameter. This parameter is applied on the web interface or with the Devolutions Web Login browser companion tool. It has no effect on Remote Desktop Manager.
User license type	Select the license type. Default is Connection Management .
Launch connection with	Sets the application that opens remote connections: Remote Desktop Manager or Devolutions Launcher. Default refers to Devolutions Launcher.
Client HttpRequest cache count	For internal use. Do not modify this value unless specified for support situation.

5.5.2.2.2 Security

5.5.2.2.2.1 Two-Factor

DESCRIPTION



This feature is only available with Devolutions Server Enterprise or Platinum licenses.

Configure **Two-Factor Authentication** in Devolutions Server to add an extra layer of security to the application.

Devolutions Server supports 9 types of 2FA. You can configure a default 2FA type for your entire organization or configure 2FA by user. When 2FA is configured, users log in with their username/password as well as a 2FA product.

HOW TO CONFIGURE 2FA FROM THE WEB INTERFACE


SETTINGS

1. To access the 2FA configuration, go to **Administration – Password Server Settings – Two-Factor**
2. Choose how you want to enforce two-factor authentication in **2FA usage**.


OPTION	DESCRIPTION
None	2FA is not enforced.
Optional per user	<p>2FA is enforced on an individual basis. The administrator chooses who uses 2FA and what product or technology they use.</p> <p>Choose this option if not all users are set up for two-factor authentication.</p>
Required	2FA is enforced for all users. A default 2FA type is set for all users.


3. Select who receives 2FA reset requests from users. You can choose to send the email to all Devolutions Server **administrators** or a **specific email**.
4. If you chose to send reset requests to an email address instead of the Devolutions Server administrators, enter the email address in **specific email**.

5. Select the 2FA types users can authenticate with. Choose as many as necessary.
6. If you chose 2FA usage as **Required** in **step 3**, choose the **Default** 2FA type.
7. Select **alternate** ways to log in. These options will be offered when users do not have access to the usual method.


ADMINISTRATION > PASSWORD SERVER SETTINGS > TWO-FACTOR 


GENERAL


2FA usage
 

Send reset email to
 

Specific email



SUPPORTED 2FA 

☒ Google Authenticator 

☒ Yubikey

☒ Email [Configure](#)

☐ SMS

☐ Duo


☐ SafeNet

☐ AuthAnvil


☐ Radius

☐ Vasco

DEFAULT

Default
 

ALTERNATE

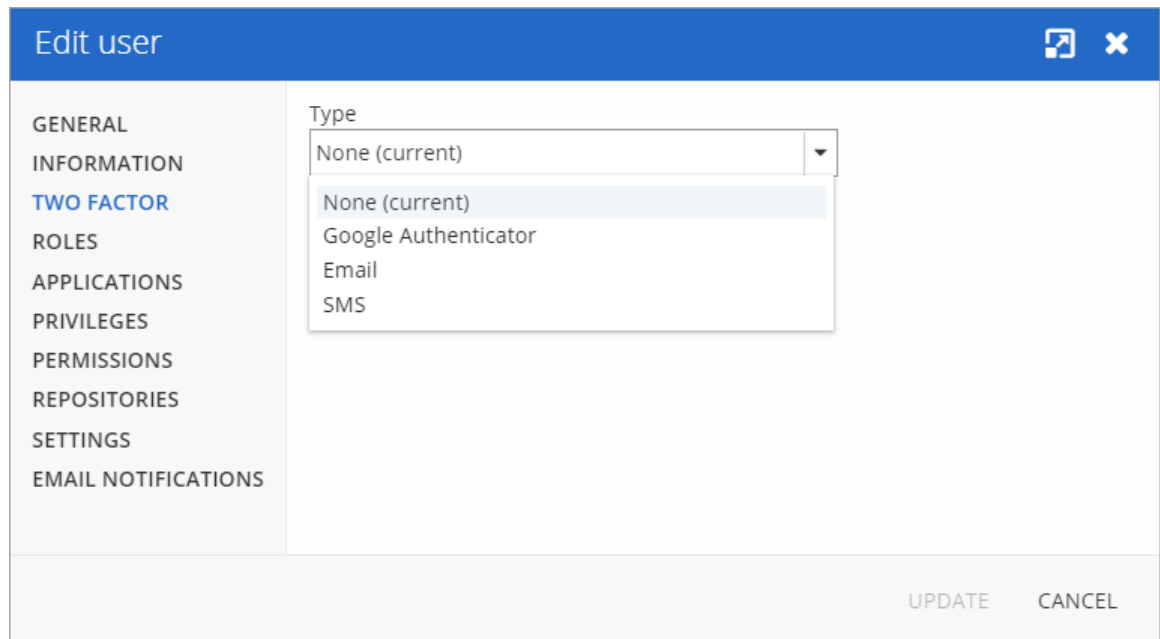
☒ Email 

☐ Backup codes

Administration - Password Server Settings - Two-Factor

8. When 2FA usage is set to **Optional per user**, the 2FA method must be configured in **Administration – Users – Two Factor** for each user. You can

also set a 2FA type on the user if they are using a product different than the default method. See [Edit Users](#) for more information.



The screenshot shows a web application window titled "Edit user". On the left is a sidebar menu with the following items: GENERAL, INFORMATION, TWO FACTOR (highlighted in blue), ROLES, APPLICATIONS, PRIVILEGES, PERMISSIONS, REPOSITORIES, SETTINGS, and EMAIL NOTIFICATIONS. The main content area shows a "Type" dropdown menu that is open, displaying the following options: "None (current)" (selected), "Google Authenticator", "Email", and "SMS". At the bottom right of the window are two buttons: "UPDATE" and "CANCEL".

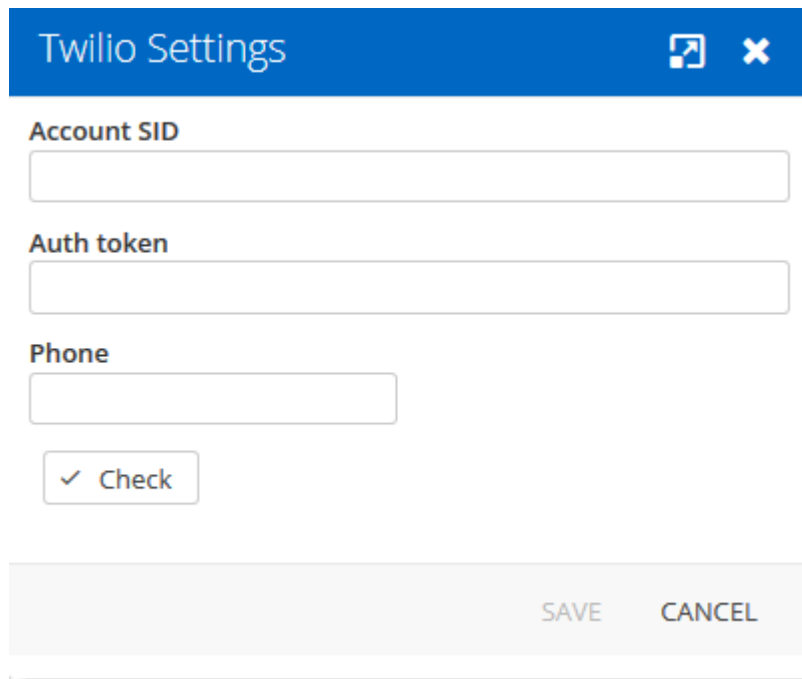
Edit User - Two Factor

OVERVIEW

The 2FA SMS will request the user to enter a code he has received on his mobile phone as its second component to access the data source.

There are two possible configuration available. To use the free version, do not fill in the Twilio settings.

The other available configuration is to configure Twilio. Please fill in the appropriate fields with the information from your Twilio subscription.

A screenshot of a 'Twilio Settings' dialog box. The dialog has a blue header bar with the title 'Twilio Settings' and two icons: a square with a diagonal line and a close 'X' button. Below the header, there are three text input fields labeled 'Account SID', 'Auth token', and 'Phone'. Below the 'Phone' field is a button with a checkmark icon and the text 'Check'. At the bottom right of the dialog are two buttons: 'SAVE' and 'CANCEL'.*Twilio Settings dialog*

OPTION	DESCRIPTION
Account SID	Account SID of your Twilio account.
Auth token	Authorization token from your Twilio account.
Phone	Phone number.

DESCRIPTION

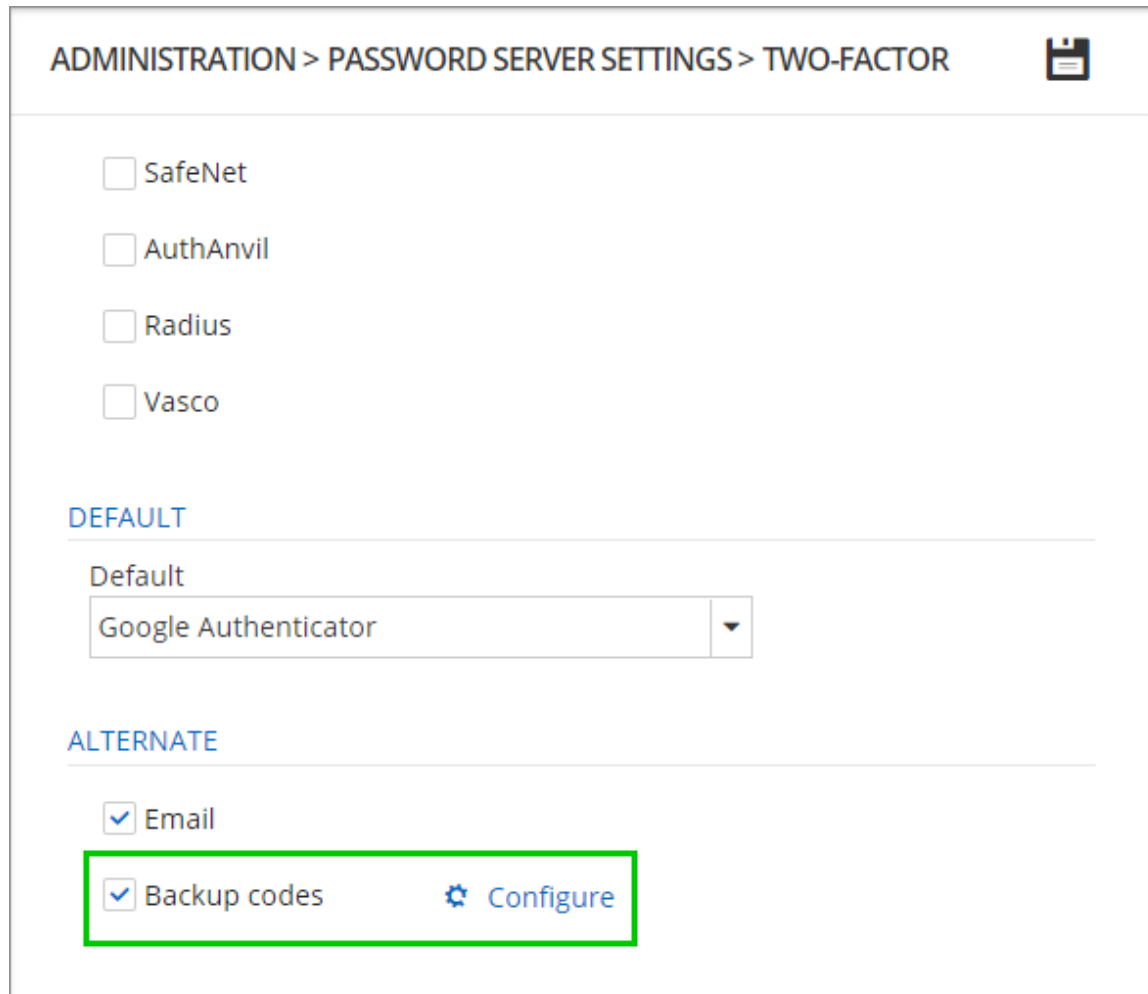
Backup codes are validation codes that provide users with one time access to Devolutions Server when they do not have access to their usual 2FA product or device. These must be generated before and kept safe in case of emergencies.


The **Administrator** enables the option and then users can generate their backup codes.

SETTINGS

ADMINISTRATOR - ENABLE BACKUP CODES

An administrator must enable backup codes as an alternate method of two-factor authentication. To turn on the option, go to **Administration – Password Server Settings – Two-Factor**.



ADMINISTRATION > PASSWORD SERVER SETTINGS > TWO-FACTOR 

☐ SafeNet


☐ AuthAnvil

☐ Radius

☐ Vasco


DEFAULT

Default

Google Authenticator 

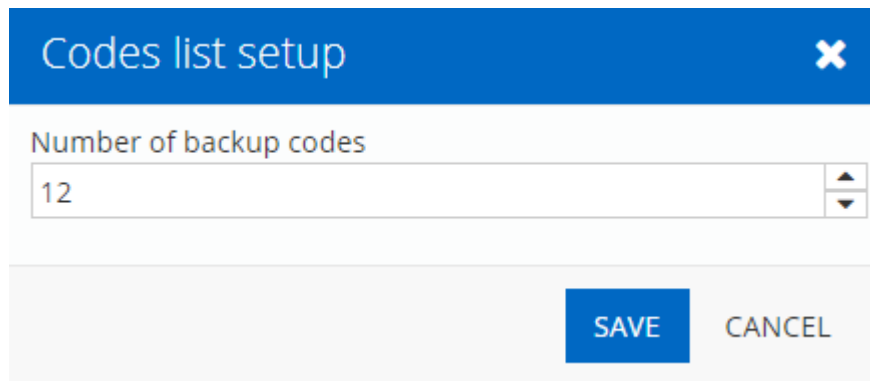
ALTERNATE

☒ Email

☒ Backup codes  [Configure](#)

Backup Codes - Two-Factor Authentication

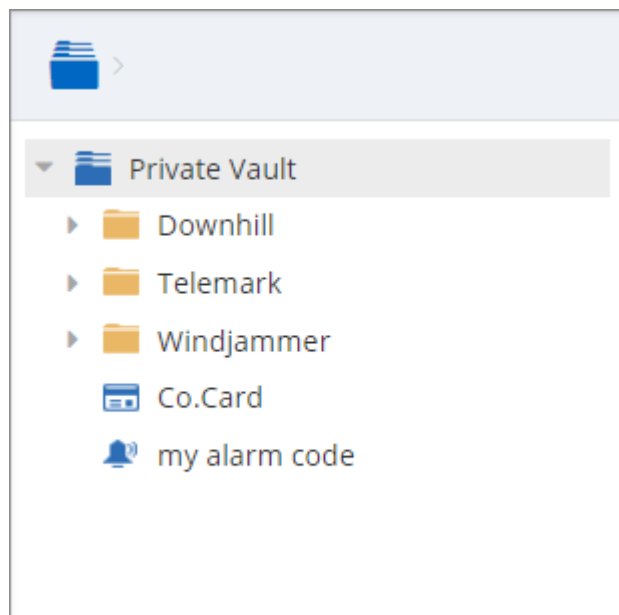
Click **Configure** to set how many backup codes a user can generate.

A dialog box titled "Codes list setup" with a blue header bar containing a close button (X). Below the header, there is a label "Number of backup codes" followed by a text input field containing the number "12" and a spinner control. At the bottom right, there are two buttons: "SAVE" (blue) and "CANCEL" (gray).

Configure the number of Backup Codes

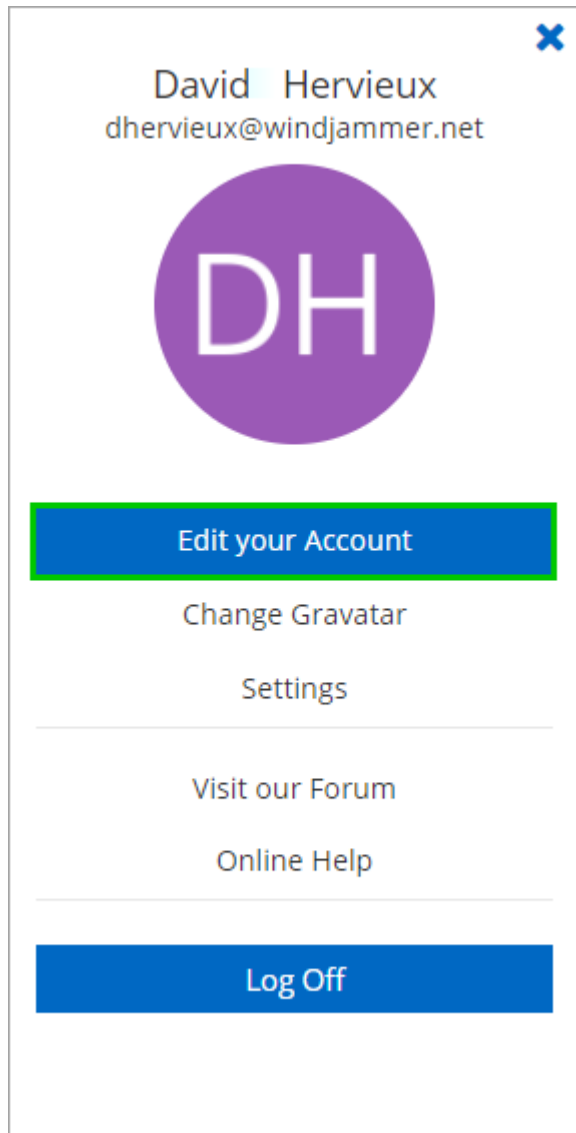
USER - GENERATE BACKUP CODES

1. To generate your backup codes, click your **avatar** in the top right corner.



Click user avatar

2. Click **Edit your Account**



Edit your Account - Account Settings

3. Click **Alternate 2FA** and then **(a)** click **Generate backup codes**. A list of backup codes are displayed **(b)**. The user can copy and paste the codes and store them elsewhere.

Edit your Account

INFORMATION

ALTERNATE 2FA

Generating new backup codes invalidate any previously generated backup codes.

a

Generate backup codes

b

Alternate Backup Codes

26373963
43656568
76896296
75223482
95644289
66496839
34396926
55372679
28698973
38929365
79397965
88577384

SAVE

CANCEL


Alternate 2FA - Generate Backup Codes


5.5.2.2.2.2 Security

DESCRIPTION

The Security section allows the administrator to configure the allowed and denied IPs addresses.

© 2020 Devolutions inc.

ADMINISTRATION > PASSWORD SERVER SETTINGS > SECURITY 

IP 

Allowed single IPs

Allowed masked IPs

Denied single IPs

Denied masked IPs

AUTO LOCK

☐ Enable automatic lock account

Attempt count

Administration - Password Server Settings - Security

SETTINGS

IP

OPTION	DESCRIPTION
Allowed Single IPs	If you wish to restrain the access to the Devolutions Server to only certain IPs address enter those here. If nothing is entered in this field all IPs address will be allowed to connect to the Devolutions Server.
Allowed Masked IPs	If you wish to restrain the access to only certain Masked IPs (dividing the host part of an IP address into a subnet

OPTION	DESCRIPTION
	and host address) on the Devolutions Server, enter those Masked IP address here.
Denied Single IPs	If you wish to deny access to the server from certain IPs address enter those in this field.
Denied Masked IPs	If you wish to deny access to the server from certain Masked IPs address (dividing the host part of an IP address into a subnet and host address) enter those in this field.


AUTO LOCK

Option	Description
Enabled auto lock	Automatically locks down the access to the Server after a predetermine number of failed attempt.
Attempt Count	Enter the number of failed attempts before locking down the Server.

5.5.2.2.2.3 GeoIP Security

DESCRIPTION

The **GeoIP Security** section section allows the administrator to set IPs restriction based on the geographical location.

ADMINISTRATION > PASSWORD SERVER SETTINGS > GEOIP SECURITY 

GENERAL ⓘ

GeoIP Mode

None ▼

User ID

License key

COUNTRIES

Select Country ▼

Administration - Password Server Settings - GeoIP Security

SETTINGS

OPTION	DESCRIPTION
GeoIP Mode	<p>Choose your method of GeoIP between:</p> <p>None: Will not be using GeoIP security</p> <p>MaxMind: Use the MaxMind's GeoIP database to look up the city, AS number and other information for an IP address. Connect to your account by entering your User ID and License Key in the appropriate field and then select the countries you wish to grant access to your Devolutions Server.</p>
User ID	User ID to connect on MaxMind.
License key	License key to connect on MaxMind.

OPTION	DESCRIPTION
Countries	Select all authorized countries to connect to the Devolutions Server instance.

5.5.2.2.2.4 Privileged Access Management

DESCRIPTION

This section is dedicated to enable and configure the Privileged Access Management.

ADMINISTRATION > PASSWORD SERVER SETTINGS > PRIVILEGED ACCESS

GENERAL

☒ Enable PAM

SECURITY

FOLDER

Access

Everyone

CREDENTIALS

View sensitive information on checkout

Everyone

Credentials brokering

Everyone

CHECK OUT

Default approval mode

none

Default reason mode

none

Default checkout time (minutes)

20

[Privileged Access Management System Permissions Page](#)

Administration - Password Server Settings - Privileged Access Management

SETTINGS

GENERAL

OPTION	DESCRIPTION
Enable PAM (Preview)	Enable the Privileged Access Management functionality.

SECURITY - FOLDER

OPTION	DESCRIPTION
Access	Possible values : <ul style="list-style-type: none">• Custom• Everyone• Never

SECURITY - CREDENTIALS

OPTION	DESCRIPTION
View sensitive information on checkout	Possible values : <ul style="list-style-type: none">• Custom• Everyone• Never
Credentials brokering	Possible values : <ul style="list-style-type: none">• Custom

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Everyone• Never

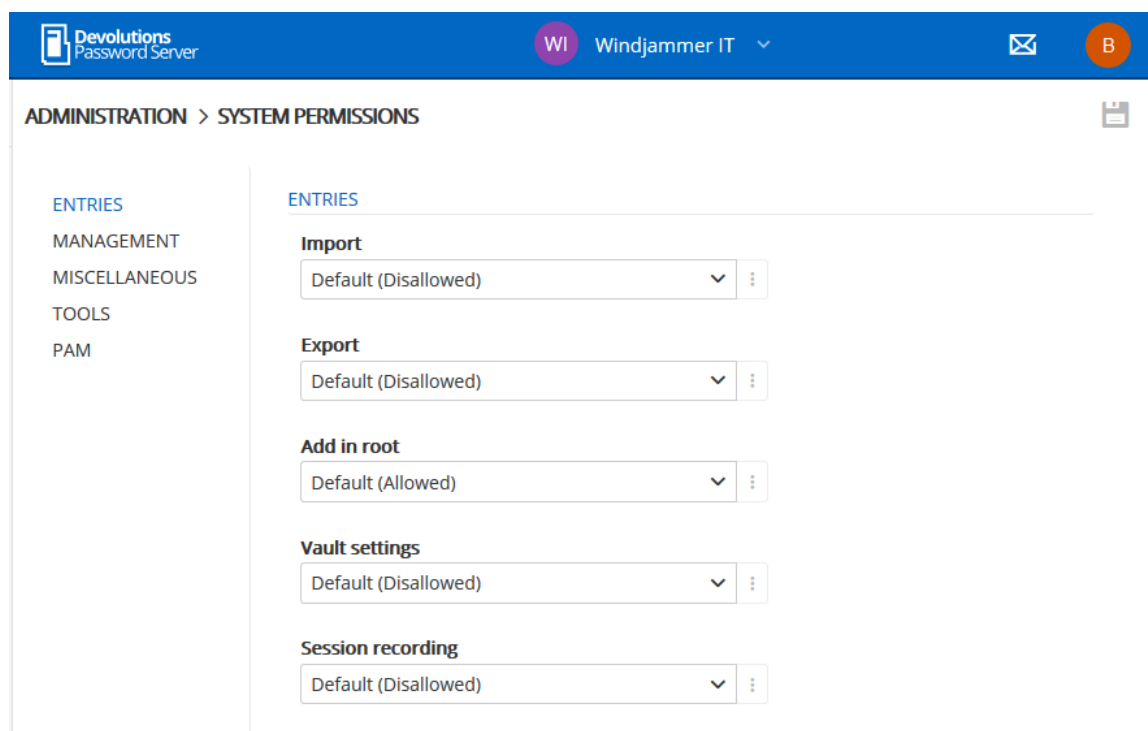
CHECK OUT

OPTION	DESCRIPTION
Default approval mode	Possible values : <ul style="list-style-type: none">• none• mandatory
Default reason mode	Possible values : <ul style="list-style-type: none">• none• mandatory• optional
Default checkout time (minutes)	

5.5.2.3 System Permissions

DESCRIPTION

The **System Permissions** allows to grant some administrative permissions to standard users without making them administrators. The **Default** setting inherits the permission set on the user or role. These are handled as you would permissions in an entry.



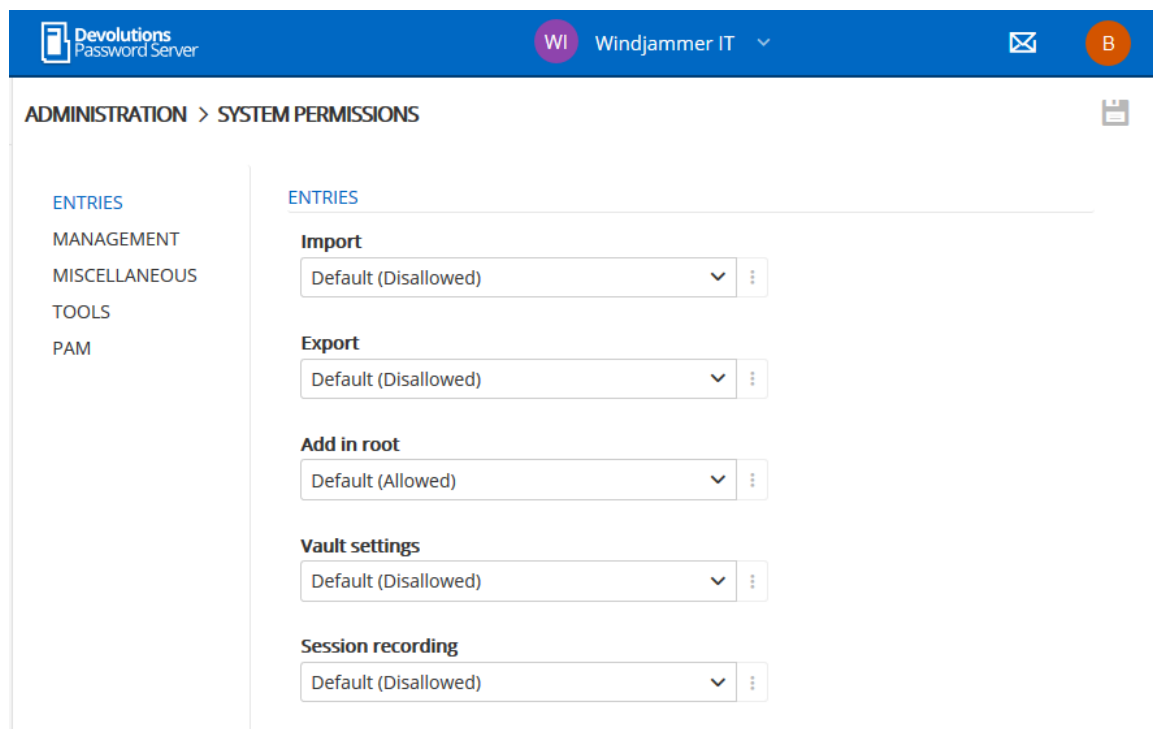
Administration - System Permissions

SYSTEM PERMISSIONS

- [Entries](#)
- [Management](#)
- [Miscellaneous](#)
- [Tools](#)
- [Privileged Access Management \(PAM\)](#)

5.5.2.3.1 Entries

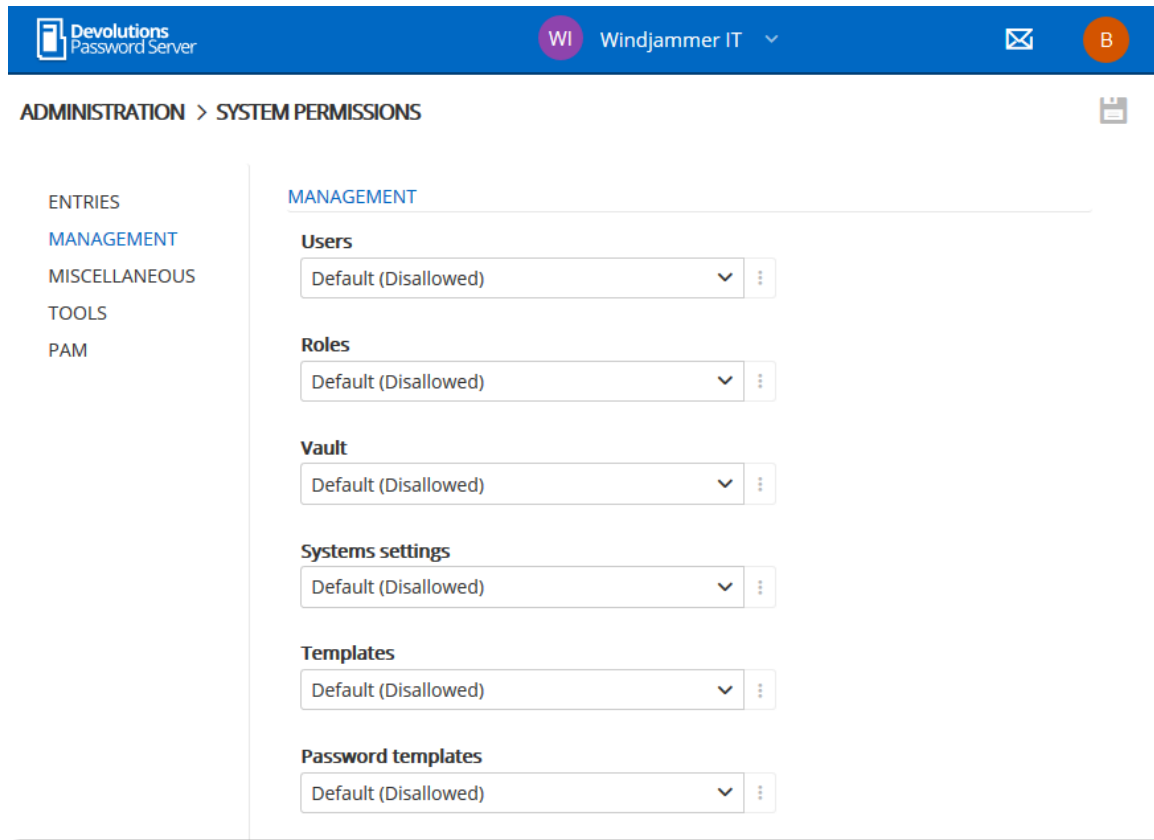
DESCRIPTION

*Administration - System Permissions*

OPTION	DESCRIPTION
Import	Restrain the import privilege to certain users.
Export	Restrain the export privilege to certain users.
Add in root	Restrain creating entries in root to certain users.
Vault settings	Restrain access to vault settings to certain users.
Session recording	Restrain access to the session recording feature.

5.5.2.3.2 Management

DESCRIPTION

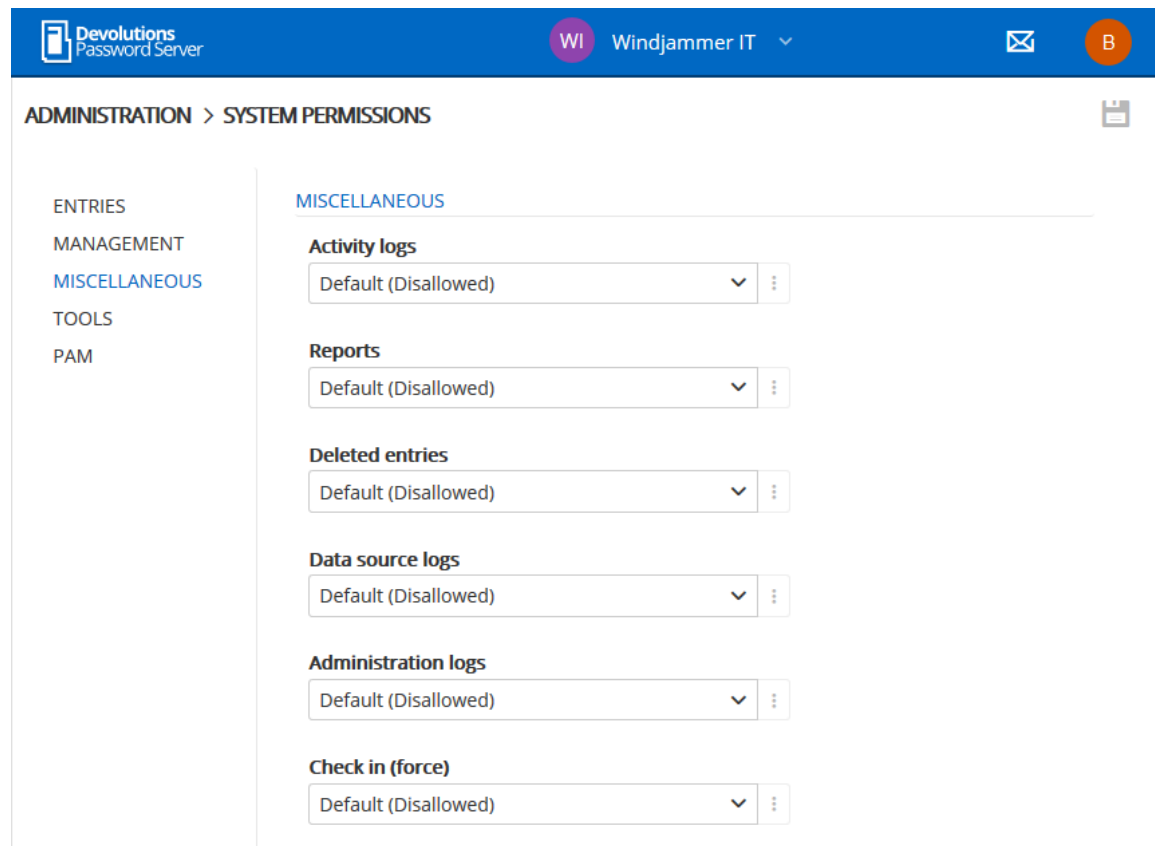


Administration - System Permissions - Management

OPTION	DESCRIPTION
Users	Allow users/roles to access the user management.
Roles	Allow users/roles to access the roles management.
Vault	Allow users/roles to access the Vault management.
System Settings	Allow users/roles to access System Settings.
Templates	Allow users/roles to create and manage templates.
Password templates	Allow users/roles to create and manage password templates.

5.5.2.3.3 Miscellaneous

DESCRIPTION



ADMINISTRATION > SYSTEM PERMISSIONS

MISCELLANEOUS

Activity logs
Default (Disallowed) ▼ ⋮

Reports
Default (Disallowed) ▼ ⋮

Deleted entries
Default (Disallowed) ▼ ⋮

Data source logs
Default (Disallowed) ▼ ⋮

Administration logs
Default (Disallowed) ▼ ⋮

Check in (force)
Default (Disallowed) ▼ ⋮

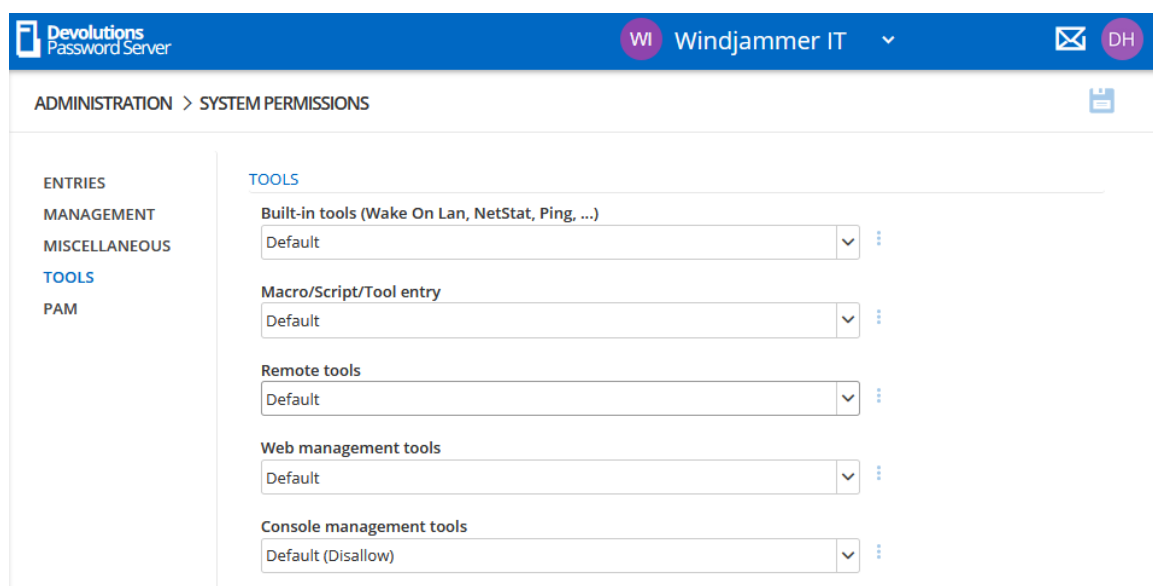
Administration - System Permissions - Miscellaneous

OPTION	DESCRIPTION
Activity logs	Allow users/roles to view the activity logs.
Reports	Allow users/roles to generate and view reports.
Deleted entries	Allow users/roles to view and restore deleted entries.
Data source logs	Allow users/roles to view the data source logs.
Administration logs	Allow users/roles to view the administration logs.

OPTION	DESCRIPTION
Check in (force)	Allow users/roles to be able to check in entries.

5.5.2.3.4 Tools

DESCRIPTION

*Administration - System Permissions - Tools*

OPTION	DESCRIPTION
Built-in tools (Wake On Lan, NetStat, Ping, ...)	Allow users/roles to use session related tools.
Macro/Script/Tool entry	Allow users/roles to use Macro/Script/Tool entries.
Remote tools	Allow users/roles to use remote tools.

OPTION	DESCRIPTION
Web management tools	Allow users/roles to use web management tools.
Console management tools	Allow users/roles to use console management tools.

5.5.2.3.5 Privileged Access Management

DESCRIPTION



To use these features you must first ensure they are enabled in the [Privileged Access Management](#) in the **Password Server Settings**.

The screenshot displays the 'ADMINISTRATION > SYSTEM PERMISSIONS' section of the Devolutions Password Server interface. On the left, a sidebar lists categories: ENTRIES, MANAGEMENT, MISCELLANEOUS, TOOLS, and PAM (which is highlighted). The main content area is titled 'PRIVILEGED ACCESS MANAGEMENT'. It contains two configuration items: 'Has Access To The PAM Section' and 'Manage Privileged Accounts'. Each item has a dropdown menu currently showing 'Default (Disallow)'. Below these items is a link labeled 'Privileged Access Management Configuration Page'.

Administration - System Permissions - PAM

OPTION	DESCRIPTION
Has Access to the PAM Section	Determine who has access to the PAM section.
Manage Privileged Accounts	Determine who can managed the Privileged accounts.

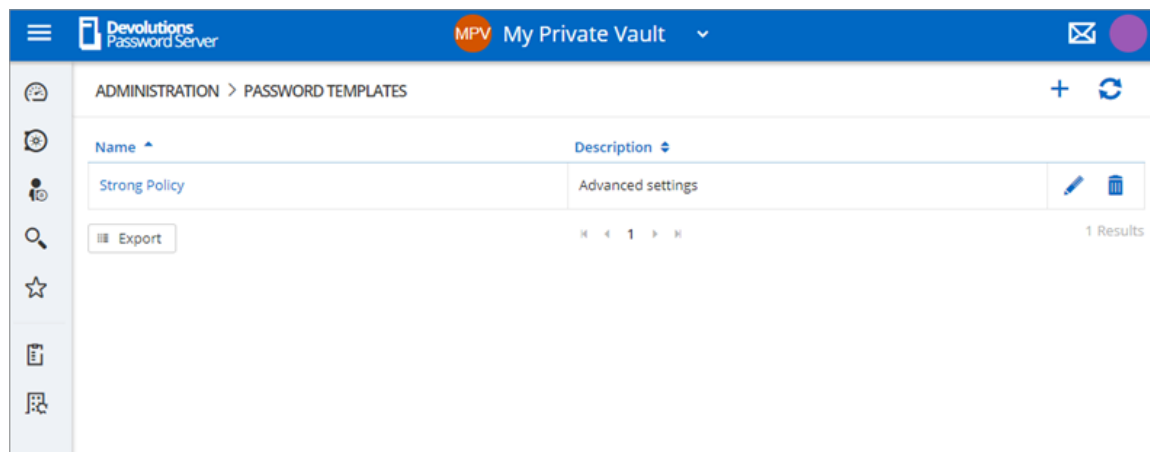
OPTION	DESCRIPTION
Privileged Access Management Configuration Page	Links you to the Configuration page of the PAM.

5.5.3 Templates

5.5.3.1 Password Templates

DESCRIPTION

The **Password Templates** allow administrators to manage password templates.



Administration - Password Templates

Password Templates

SECURITY

Name

Strong Policy

Mode

Advanced settings

Password length

20

☒ Upper-case (A, B, ...)
☐ Underline (_)
☐ High ANSI characters
☐ Minus (-)
☐ Brackets ([,], <, >)

2

0

0

0

0

☒ Digits (0, 1, 2, ...)

☒ Special (!, \$, %, &, ...)

☒ Lower-case (a, b, c, ...)

☐ Space ()

☐ XML Compliant

1

1

1

0

Include the following characters

A

1

Exclude the following characters:

#, \$, <, !, |

PREVIEW

Password Count

30

UPDATE

CANCEL

Password Templates

OPTION	DESCRIPTION
Name	Name of the Password Template.
Mode	<ul style="list-style-type: none"> • Default • Advanced settings • Readable password • Use a pattern • Pronounceable password • Strong password
Upper-case (A, B, C, ...)	Will include uppercase letters for password generation.




















OPTION	DESCRIPTION
Underline (_)	Will include the underline (_) character for password generation.
High ANSI characters	Will include characters from ' ' to U255 (excluding U255) for password generation.
Minus (-)	Will include the minus (-) character for password generation.
Brackets ([,], (,), <, >)	Will include brackets characters for password generation.
Digits (0, 1, 2, ...)	Will include digits for password generation.
Special (!, \$, %, &, ...)	Will include special characters for password generation.
Lower-case (a, b, c, ...)	Will include lowercase letters for password generation.
Space ()	Will include the space character for password generation.
XML Compliant	Will generate XML compliant passwords.
Also include the following characters	Add any other characters to be include for password generation.
Exclude the following characters	The characters listed in this field will not be used for password generation.
Password count	Number of passwords that will be generated.
Include the following characters	Forcefully including characters inside the password.

OPTION	DESCRIPTION
Exclude the following characters	Forcefully excludes characters from the password.

5.5.3.2 Templates

DESCRIPTION

The **Templates** allow administrators to manage entry templates. With this you can set preferences to how entries information will be filled when creating them.

ADMINISTRATION > TEMPLATES		 
Name ^	Type	
 MyFolderTemplate	Group	  
 MyRDPTemplate	RDPConfigured	  
 OtherFolderTemplate	Group	  
 Display value only ▾		  1  
		3 Results

5.5.4 Backup

5.5.4.1 Backup Manager

DESCRIPTION

The **Backup Manager** section allow administrators to configure the parameters to backup the database and the web application folder.

The screenshot shows the 'ADMINISTRATION > BACKUP MANAGER' page in the Devolutions Password Server. The page is divided into several sections:

- DATABASE CONFIGURATION:** Includes a checkbox for 'Enable database backup' and a text field for 'Backup database file path'.
- WEB CONFIGURATION:** Includes a checkbox for 'Enable web backup' and a text field for 'Backup web file path'.
- SCHEDULE:** Includes a checkbox for 'Notify Administrator on backup failed', a 'Backup start time' field (showing 11/13/2018 05:43 AM), and a 'Repeat every' section with 'Days' (0) and 'Hours' (1) dropdowns.
- ADVANCED:** Includes a 'Database backup SQL timeout (Minutes)' field (1), a 'Keep number of backups' field (1), and a checkbox for 'Copy only database backup'.

Administration - Backup Manager

SETTINGS

BUTTON	DESCRIPTION
Save	Save the latest modifications of the Backup schedule options.
Backup Now	Create immediately a backup of the SQL database and/or the web application folder.

DATABASE CONFIGURATION

OPTION	DESCRIPTION
Enable database	Activate the backup of the SQL database.

OPTION	DESCRIPTION
backup	
Backup database file path	<p>The path to the folder where the backup of the SQL database will be saved. We recommend to use a shared network folder with proper permissions set on it to be able to save the backup file.</p> <p>Note: As the backup command is running on the SQL Server, this path must exist on the SQL Server or accessible from that SQL Server.</p>

WEB CONFIGURATION

OPTION	DESCRIPTION
Enable web backup	Activate the backup of the web application.
Backup web file path	The path to the folder where the backup of the web application will be saved. We recommend to use a shared network folder with proper permissions set on it to be able to save the backup file.

SCHEDULE

OPTION	DESCRIPTION
Notify Administrator on backup failed	Will send an email when the backup fails. The Email feature must be enabled in the Server Settings in order to work. For more information, please see Email Settings .

OPTION	DESCRIPTION
Backup start time	Date and time when the backup will be automatically started.
Repeat every	The time interval when the backup will be repeated.


ADVANCED

OPTION	DESCRIPTION
Database backup SQL timeout (Minutes)	Number of minutes before a timeout in the SQL instance.
Keep number of backups	Number of the backup that will be kept in the backup folder.
Copy only database backup	A SQL Server backup that is independent of the sequence of conventional SQL Server backups. For more information, please see https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/copy-only-backups-sql-server .

5.5.4.2 Backup List

DESCRIPTION

The **Backup List** section displays the list of the backup that have been taken.

ADMINISTRATION > BACKUP LIST 

Start Date/Time	End Date/Time	Notes	Filename	Database Filename	Success
10/22/2018 1:00 PM	10/22/2018 1:00 PM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 11:00 AM	10/22/2018 11:01 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 9:00 AM	10/22/2018 9:00 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 7:00 AM	10/22/2018 7:00 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 5:00 AM	10/22/2018 5:00 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 3:00 AM	10/22/2018 3:00 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/22/2018 1:00 AM	10/22/2018 1:00 AM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/21/2018 11:00 PM	10/21/2018 11:00 PM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓
10/21/2018 9:00 PM	10/21/2018 9:00 PM	Database backup co...	C:\Users\Administrat...	C:\Users\Administrat...	✓

1274 Results

Administration - Backup List

COLUMN	DESCRIPTION
Start Date/Time	Date and time when the backup process was started.
End Date/Time	Date and time when the backup process was stopped.
Notes	Message to inform the completion or the fail of the backup.
Filename	Path and name of the web application backup file.
Database Filename	Path and name of the SQL database backup file.
Success	<p>A check mark will indicate a successful backup.</p> <p>An X will indicate that the backup has failed.</p>

5.5.5 Logs

5.5.5.1 Cleanup Logs

DESCRIPTION

The Cleanup Logs functionality will allow to archive logs available in the database that are older than the selected period. And it can also delete these archived logs based on the selected time limit in the parameters.

ADMINISTRATION > CLEANUP LOGS

GENERAL

☒ Enable automatic cleanup

Run every day at

03:24 PM *🕒

CONFIGURATION

☒ Use Archive

Archive logs older than


Six months

Delete archived logs older than

One year

☐ Skip archiving and permanently delete

Delete logs older than

 Advanced

Custom configuration is in use

Cleanup logs

OPTION	DESCRIPTION
Enable automatic cleanup	Enable the automatic cleanup logs feature to automatically archive and delete logs.
Run every day at	Set the time when the feature will run.

OPTION	DESCRIPTION
Use Archive	If enable, the job will archive and delete logs based on the period selected in the two drop down lists.
Archive logs older than	<p>Will archive logs that are older than the selected value in the drop down list.</p> <p>Possible choices :</p> <ul style="list-style-type: none">One monthThree monthsSix monthsOne year
Delete archived logs older than	<p>Will delete all archived logs that are older than the selected value in the drop down list.</p> <p>Possible choices :</p> <ul style="list-style-type: none">Three monthsSix monthsOne yearTwo years
Skip archiving and permanently delete	If enable, will not archive the logs and will permanently delete them
Delete Logs older than	<p>Will permanently delete all logs older than the selected value in the drop down list.</p> <p>Possible choices :</p> <ul style="list-style-type: none">One monthThree monthsSix monthsOne yearTwo years
Advanced	Advanced configuration if for configuring the archiving and deletion operation on each logs separately.

5.5.5.1.1 Advanced configuration

DESCRIPTION

The advanced configuration allows to set individual clean up parameters for all different logs of Devolutions Server.

Advanced Configuration

GENERAL

☒ Use custom configuration

CONFIGURATION

☒ **Use Archive**

Archive logs older than
One month

Delete archived logs older than
Three months

☐ **Skip archiving and permanently delete**

Delete logs older than

OK Cancel

Cleanup Logs - Advanced configuration

LOGS	DESCRIPTION
Backup Logs	Logs related to the Backup Manager .

LOGS	DESCRIPTION
Connection Logs	Logs related to all operations on entries like viewing a password, opening an entry, etc.
Login Attempt	Logs related to failed login attempts to Devolutions Server.
Login History	Logs related to all successful logins to Devolutions Server.
Message Logs	Logs related to data source logs of Devolutions Server.
PAM Logs	Logs related to the Devolutions Server PAM feature.

GENERAL	DESCRIPTION
Use custom configuration	Allow to set specific archiving and deletion parameters for the selected log.

CONFIGURATION	DESCRIPTION
Use archive	Use the archive operation to clean the logs.
Archive logs older than	<p>Will archive logs that are older than the selected value in the drop down list.</p> <p>Possible choices :</p> <ul style="list-style-type: none">One monthThree monthsSix monthsOne year

CONFIGURATION	DESCRIPTION
Delete archive logs older than	<p>Will delete all archived logs that are older than the selected value in the drop down list.</p> <p>Possible choices :</p> <p>Three months Six months One year Two years</p>
Skip archiving and permanently delete	If enable, will not archive the logs and will permanently delete them
Delete Logs older than	<p>Will permanently delete all logs older than the selected value in the drop down list.</p> <p>Possible choices :</p> <p>One month Three months Six months One year Two years</p>

5.6 Role Based Security

DESCRIPTION

Devolutions Server role-based security allows to create a granular protection system that is quite flexible. However, flexibility comes at a price and sometimes making the wrong choices could increase the time involved in managing the system.

The following recommendations are based on our experience with the system and the ideas shared by our community. Follow these guidelines, as they will help you to use the Devolutions Server role-based security efficiently.

Here are the main key points of the role based security:

- **Security is inherited:** child items and folders are covered by a parent folder's security.
- **Permissions can be overridden:** a permission set on a sub folder will override the parent item's permission.

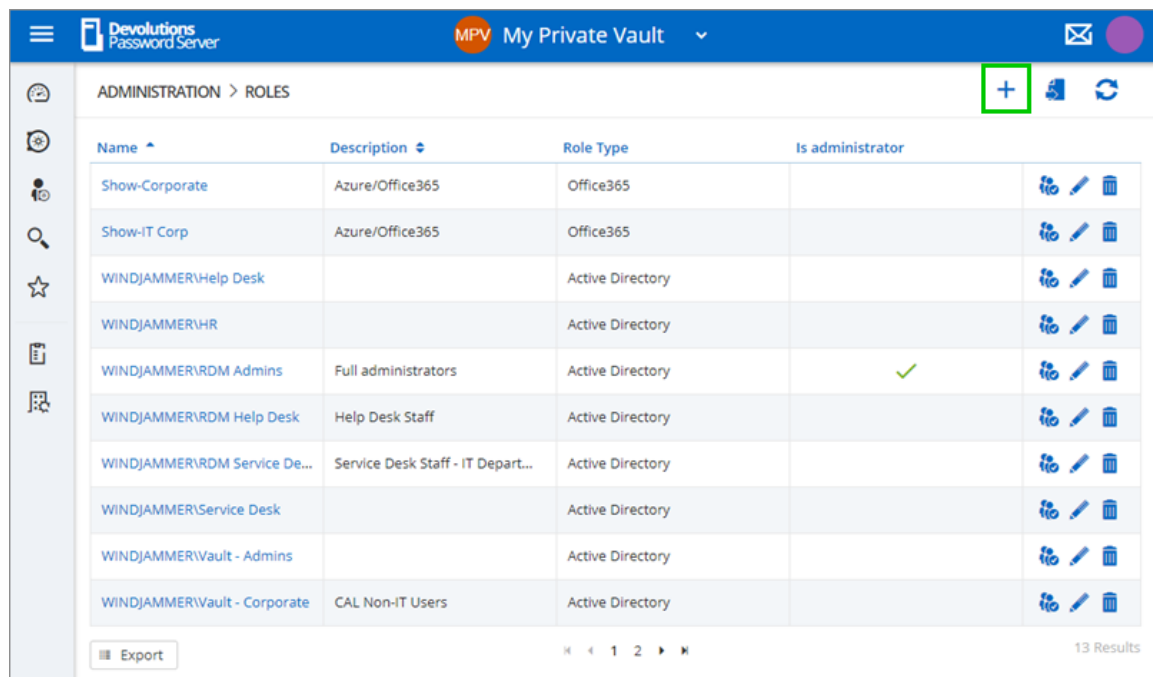
- **Permissions are granular:** multiple permissions can be set on entries at once.

ROLE CONFIGURATION

When using Devolutions Server role-based security, roles are mostly used to control user access for multiple users at once.

CREATE THE ROLE

To create roles, navigate to **Administration – Roles**, then click **+ Add Role**.



Create a Role

All settings can be left to default unless the role contains only administrators. In this case, check the **Administrator** box when configuring the role. Enter a name for the role, then click **OK**. For Active Directory groups, the domain must be provided like the following.

Roles

GENERAL

VAULTS

SETTINGS

EMAIL NOTIFICATIONS

Name *


WINDJAMMER/RDM Users *

Description

☐ **Is administrator**

OK CANCEL

Configure a Role

To assign users to the role, click , then check the Is Member box of the respective user. With a role created from an Active Directory group, there is no need to assign users as it is automatically managed by Devolutions Server.

Role Assignment - Service Desk

✕ Unselect All ✓ Select All

Name ^	Description	Is administrator	Is member
_Administrator		✓	<input type="checkbox"/>
bill@windjammer.loc	Bill Preston	✓	<input checked="" type="checkbox"/>

1 2 Results

UPDATE CANCEL

Assign a user to the Role

USER CONFIGURATION

USER TEMPLATE

It is possible to change the default user template. To do so, navigate to **Administration – System Settings – User Template**. These settings control the default settings of a new user. The best practice is to disable all privileges.

CREATE THE USER

To create users, navigate to **Administration – Users**, then click **+ Add User**. Enter a **Login** for the user, select the **User** type and enter an email address.

Add user

GENERAL

Authentication type
Custom (Devolutions)

User

Password

User type
Read only user

User license type
Default

☒ Enabled

☐ Must change password at next logon

INFORMATION

First name

Last name

Email

ADD CANCEL

Create a user

A user can be assigned to multiple roles at once by checking the **Is Member** box of the respective roles in the **Roles** section of the **User Management**. As part of the Active Directory integration, there is no need to assign users to those roles as it is automatically managed by Devolutions Server.

Edit user

GENERAL
INFORMATION
TWO FACTOR
ROLES
APPLICATIONS
VAULTS
SETTINGS
EMAIL NOTIFICATIONS

Only custom roles can be manually assigned.

X Unselect All ✓ Select All

Name ^	Description	Role Type ^	Is member
WINDJAMMER\Vault ...	Password Vault Users	Active Directory	<input type="checkbox"/>
WINDJAMMER\Vault ~...		Active Directory	<input type="checkbox"/>
WINDJAMMER\RDM S...	Service Desk Staff - IT...	Active Directory	<input type="checkbox"/>
Show-IT Corp	Azure/Office365	Office365	<input type="checkbox"/>
WINDJAMMER\Vault ~...	Groups from IT Depa...	Active Directory	<input type="checkbox"/>
Show-Corporate	Azure/Office365	Office365	<input type="checkbox"/>
WINDJAMMER\RDM ...	Full administrators	Active Directory	<input type="checkbox"/>
WINDJAMMER\Vault ~...	CAL Non-IT Users	Active Directory	<input type="checkbox"/>
WINDJAMMER\HR		Active Directory	<input type="checkbox"/>
WINDJAMMER\Service...		Active Directory	<input type="checkbox"/>

UPDATE CANCEL

ADMINISTRATORS

Administrators can do everything, regardless of the security. These users are usually the chief officers and senior management.

RESTRICTED USERS

Restricted users have limited access to resources. They usually have the **Add** and **Edit** rights only. These users can be mid or first level executives, such as service desk and help desk.

USERS

Users also have limited access to resources much like **Restricted users**. However, **Users** have by default the **Add**, **Edit** and **Delete** rights and can perform these actions on all unsecured entries.

READ ONLY USERS

Read only users can only view and use resources, but cannot edit them. These users are usually external consultants.

SELECT THE APPROPRIATE USER TYPE

When creating users, some key points must be taken into consideration. Ask yourself the following questions while configuring a new user:

➤ **Should they be able to access any resource without restriction?**

- ✓ **Administrators** can access any resource without restriction.
- ✓ Make a user administrator by selecting **Administrator** as the **User type** when creating the user.

The screenshot shows the 'Add user' dialog box. The left sidebar contains the following menu items: GENERAL, INFORMATION, TWO FACTOR, ROLES, APPLICATIONS, VAULTS, SETTINGS, and EMAIL NOTIFICATIONS. The main content area is divided into two sections: GENERAL and INFORMATION. In the GENERAL section, the Authentication type is set to Domain. The User field contains david@windjammer.loc. The User type is set to Administrator and the User license type is set to Default. There is a checked Enabled checkbox and an unchecked Must change password at next login checkbox. In the INFORMATION section, the First name and Last name fields are empty, and the Email field contains david@windjammer.loc. At the bottom right of the dialog are ADD and CANCEL buttons.

Administrator user

➤ **Should they be able to add, edit, or delete entries?**

- ✓ Make a **Restricted user** by selecting **Restricted user** as the **User type** when creating the user.

✓ Set up manually which rights are granted to the user.

Add user

GENERAL

Authentication type: Domain

User: ted@windjammer.loc

User type: Restricted user

User license type: Default

☒ Enabled

☐ Must change password at next logon

RIGHTS

☐ Add ☐ Edit ☐ Delete

☐ Add in root ☐ Move

INFORMATION

First name:

Last name:

Email: ted@windjammer.loc

ADD CANCEL

Restricted user

ENTRY CONFIGURATION

Access is granted or denied to users by setting permission on entries. **Permissions** can be set to users or roles. The best practice is to grant permissions to roles to control access for multiple users at once.

To set permissions on an entry, edit any entry, then navigate to the **Security – Permissions** section.

Wayk Now

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

Permission
Default

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View
Inherited

Roles: WINDJAMMER\RDM Service Desk

Edit
Inherited (Never)

Delete
Inherited (Never)

View password
Inherited (Never)

Connect (Execute)
Inherited (Allowed)

UPDATE CANCEL

Entry's Permissions

Permissions are usually set on folders, and apply to all child entries. A best practice is to set all the permissions of the root folder to **Never**. As a result, all permissions of all entries are denied by default.

Root

GENERAL
SECURITY

PERMISSIONS

Allow offline
True

Add in root
Never

Root properties
Never

Permission
Never

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View
Default

Add
Default

Edit
Default

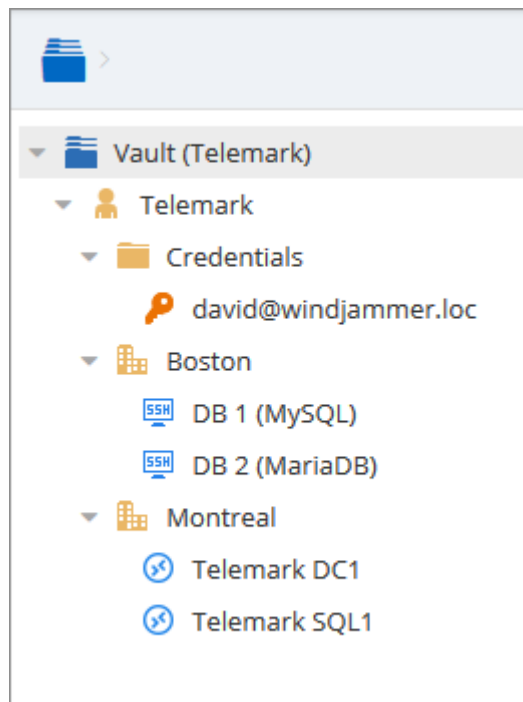
UPDATE CANCEL

Root Permissions

Access is denied to users by expressly granting the access to other users. In other words, all users that are not on the list of a permission have the access denied.

For a user to have access to a sub folder, the user must have at least the **View** permission on all parent folders.

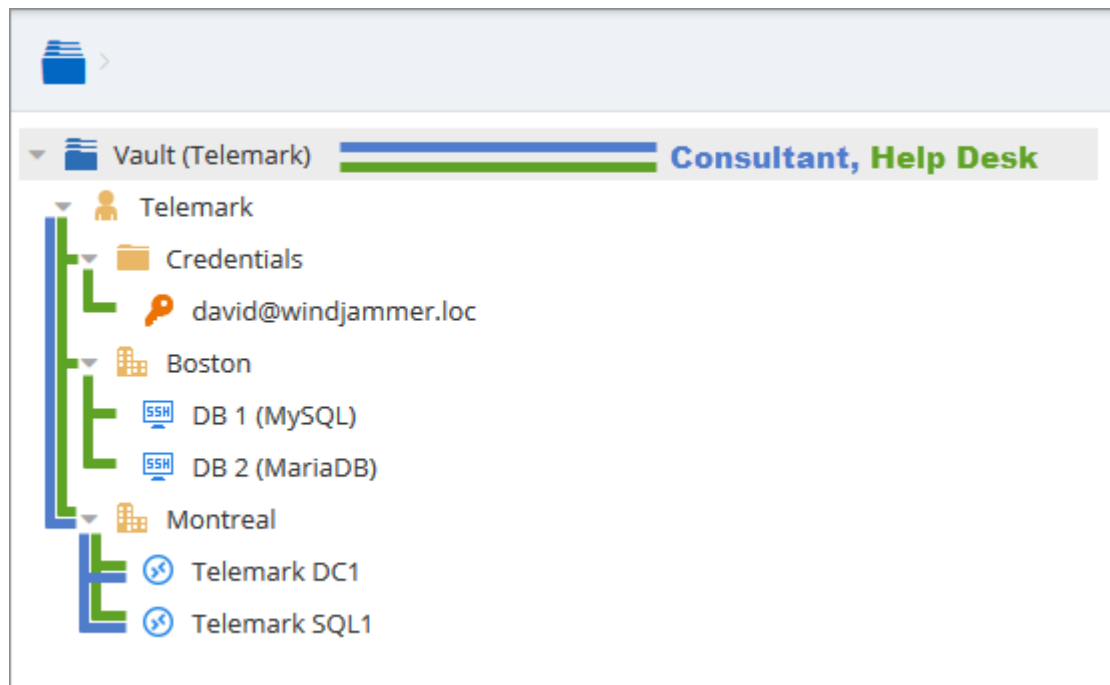
Consider the following structure:



Sample Structure

There are three levels of folders: the root, Telemark, and child items of Telemark.

Suppose that a user, such as a consultant, must have access to the Montreal folder only. The consultant must be granted the **View** permission on the Telemark folder as well. However, granting the **View** access to the Telemark folder gives to the consultant the permissions to view all child items of Telemark. To deny the **View** permissions for the consultant on specific child items, the **View** permissions of these items must be expressly set for other users.



Permissions Structure

5.6.1 Permissions

DESCRIPTION

The **Permissions** panel can be found in every entry properties in the **Security - Permissions** section.

It is also possible to allow administrators to grant administrative permissions to standard users without making them administrators with [System Permissions](#).

The role-based permissions system can give a very accurate control of the security. Here is an overview of the permissions window:

Folder - Workstation

GENERAL
MORE
SECURITY
USER
INTERFACE
EMAIL
NOTIFICATIONS
ADVANCED

Permission
1 Custom

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View
2 Everyone

Add
Custom
3

Roles: WINDJAMMER\Vault - IT Corp
4

Edit
Custom

Roles: WINDJAMMER\Vault - IT Corp

Delete
Default

View password
Custom

Roles: WINDJAMMER\Vault - IT Corp

Execute
Default

UPDATE CANCEL

Permissions Panel

OPTION	DESCRIPTION
1. Permission	<p>Sets the permission mode. This must be set to Custom in order to change the discrete permissions below. Select between:</p> <ul style="list-style-type: none"> • Inherited (Default): will inherit the permissions from the parent groups. • Custom: lets you specify a custom value for each of the permission. • Everyone: everyone will be granted all the permissions below.

OPTION	DESCRIPTION
	<ul style="list-style-type: none">• Never: no one but the administrators will be granted the permissions
2. Discrete permissions	<p>Lets you choose who you want to grant permissions to. These combo boxes are available only if the above Permission combo box is set to Custom. Select between:</p> <ul style="list-style-type: none">• Inherited (Default): will inherit the permissions from the parent groups/folders.• Custom: lets you specify a custom value for the permission.• Everyone: everyone will be granted the permission• Never: no one but the administrators will be granted the permission.
3. Users / Roles selector	<p>Lets you select Users / Roles to be granted the permission. Available only if the permission is set to Custom.</p>
4. Current permission	<p>Displays the granted permission for the current entry.</p>

GENERAL

Folder - Workstation

GENERAL
MORE
SECURITY
USER
INTERFACE
EMAIL
NOTIFICATIONS
ADVANCED

Permission
Custom

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View
Everyone

Add
Custom

Roles: WINDJAMMER\Vault - IT Corp

Edit
Custom

Roles: WINDJAMMER\Vault - IT Corp

Delete
Default

View password
Custom

Roles: WINDJAMMER\Vault - IT Corp

Execute
Default

UPDATE CANCEL

Permissions - General

OPTION	DESCRIPTION
Permission	Sets the permission mode. It must be set to Custom in order to change the permissions individually.
View	Allow users/roles to view entries.
Add	Allow users/roles to add entries
Edit	Allow users/roles to edit entries.
Delete	Allow users/roles to delete entries.

OPTION	DESCRIPTION
View password	Allow users/roles to view entry password .
Connect (Execute)	Allow users/roles to open entries.

SECURITY

Folder - Workstation

GENERAL
MORE
SECURITY
USER
INTERFACE
EMAIL
NOTIFICATIONS
ADVANCED

Permission
Custom

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

Edit permissions
Default

Entry history
Default

Password history
Default

UPDATE CANCEL

Permissions - Security

OPTION	DESCRIPTION
Edit permissions	Allow users/roles to edit permissions.
Entry history	Allow users/roles to view and use entry history .
Password History	Allow users/roles to view the Password History .

MORE

Folder - Workstation

GENERAL
MORE
SECURITY
USER
INTERFACE
EMAIL
NOTIFICATIONS
ADVANCED

Permission

Custom

GENERALSECURITYMOREATTACHMENTSDOCUMENTATION

Remote tools

Default

Inventory

Default

UPDATE CANCEL

Permissions - More

OPTION	DESCRIPTION
Remote tools	Allow users/roles to use Remote Tools .
Inventory	Allow users/roles to use the Inventory Report tool.

ATTACHMENTS

Folder - Workstation

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

Permission
Custom

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View attachments
Default

Add/edit/delete attachments
Default

UPDATE CANCEL

Permissions - Attachment

OPTION	DESCRIPTION
View attachments	Allow users/roles to view attachments.
Add/edit/delete attachments	Allow users/roles to add/edit/delete attachments.

DOCUMENTATION

Folder - Workstation

GENERAL
MORE
SECURITY
USER INTERFACE
EMAIL NOTIFICATIONS
ADVANCED

Permission
Custom

GENERAL SECURITY MORE ATTACHMENTS DOCUMENTATION

View documentation
Everyone

Edit documentation
Default

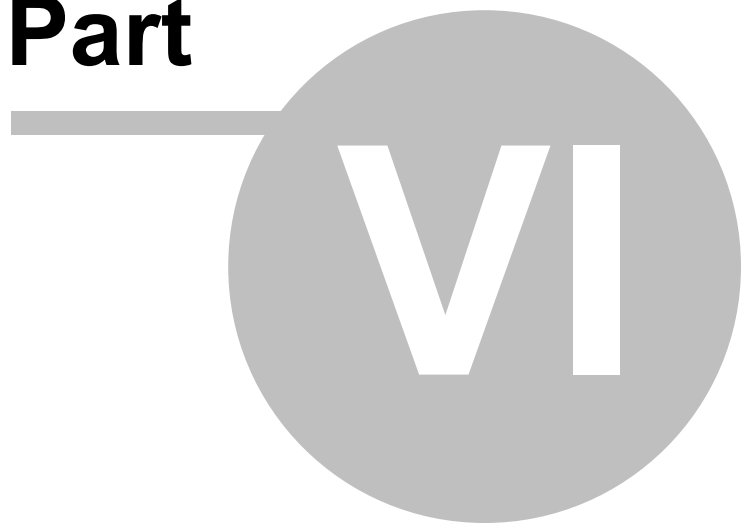
UPDATE CANCEL

Permissions - Documentation

OPTION	DESCRIPTION
View documentation	Allow users/roles to view documentation.
Edit documentation	Allow users/roles to edit documentation.

Privileged Access Management

Part



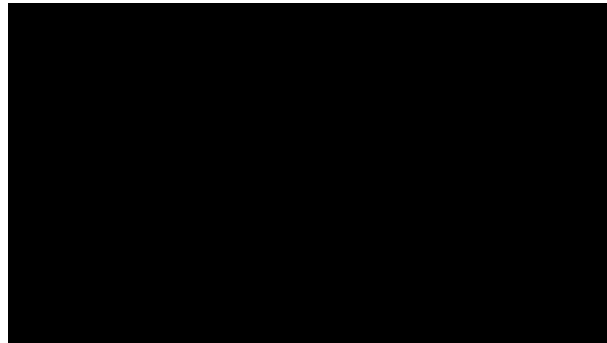
6 Privileged Access Management

DESCRIPTION

Devolutions Privileged Access Management solution provides all the following features. It is specifically designed to meet the needs of SMBs, providing enterprise-grade features to bring a level of protection usually only afforded to large organizations while at the same time being robust, easy to deploy and affordable.

1. Ease of deployment and management
2. Secure password vault
3. Logging and reporting
4. Built-in two-factor authentication
5. Access brokering
6. Role-based access control

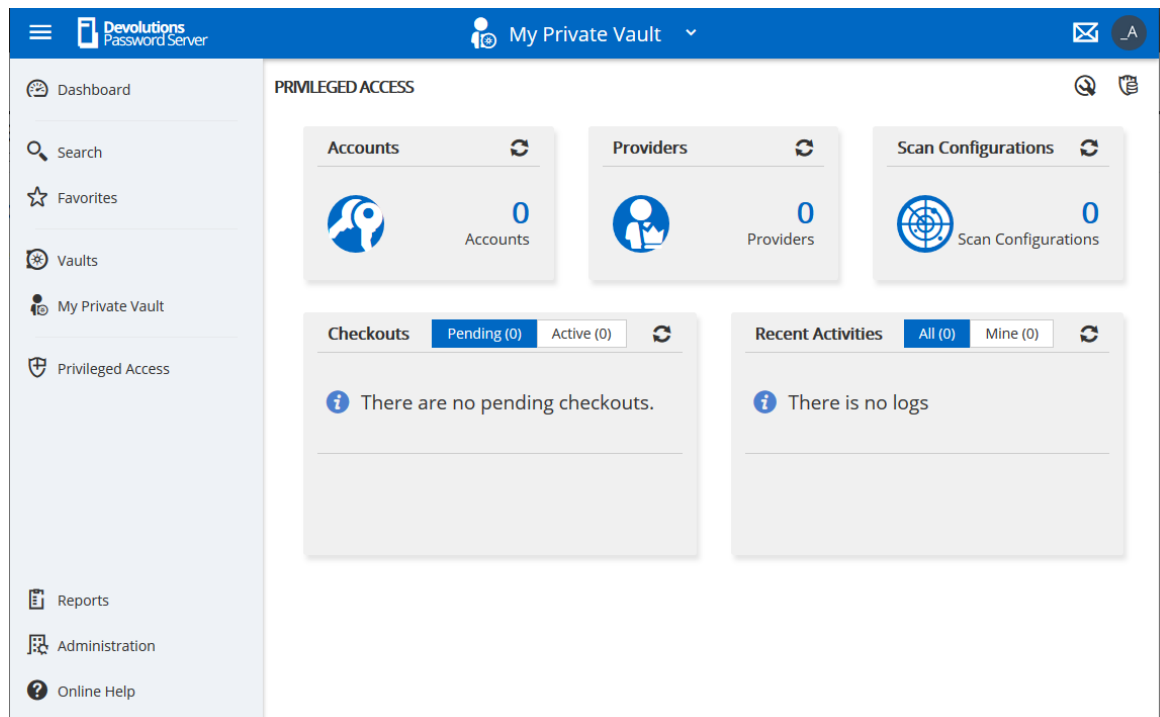
For an overview of the Devolutions Privileged Access Management, please watch the following video.



PAM Preview

PRIVILEGED ACCESS DASHBOARD

The Privileged Access Dashboard provides a quick overview of the available **Accounts**, **Providers**, **Scan Configurations**, current **Checkouts** and the **Recent Activities**.



Privileged Access Management Dashboard

6.1 Getting Started

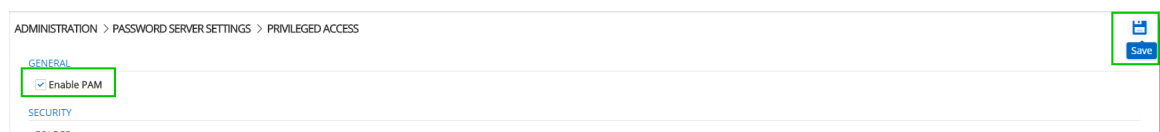
DESCRIPTION

In this topic, you will find the steps on how to get started with the **Privileged Access Management** features in Devolutions Server.

First, you will need to be logged as an administrator in your DPS.

PAM SETTINGS CONFIGURATION

1. Head to **Administration -> Password Server Settings -> PAM**.
2. Check **Enable PAM** and click the **Save** button in the top right to make the PAM side-panel appear on the left.



Enabling PAM

3. Configure the default settings for the [checkout system](#), [credentials brokering](#), [sensitive information access](#), default checkout times and synchronizations. The **Custom** setting allows role-based access control.

The screenshot shows the 'SECURITY' configuration page in Devolutions Server. It is divided into several sections:

- FOLDER**: 'Access' is set to 'Everyone'.
- CREDENTIALS**: 'View sensitive information on checkout' is set to 'Everyone'. 'Credentials brokering' is set to 'Everyone'.
- CHECK OUT**: 'Default approval mode' is set to 'mandatory'. 'Default reason mode' is set to 'optional'. 'Default checkout time (minutes)' is set to '240'.
- SYNCHRONIZATION**: 'Check synchronization status every (minutes)' is set to '360'.

4. Next, head to **Administration -> System Permissions -> PAM**.

5. Configure the accesses to the PAM system for the users/admins and manage privileged accounts rights on who can edit the privileged entries. Then, click **Save**.

The screenshot shows the 'ADMINISTRATION > SYSTEM PERMISSIONS' page. The 'PAM' tab is selected in the left sidebar. The 'PRIVILEGED ACCESS' section is highlighted with a green box and contains the following settings:

- 'Has Access To The PAM Section' is set to 'Custom'.
- 'Users:' lists 'kelly@windjammer.loc', 'maurice@windjammer.loc', 'bob@windjammer.loc'.
- 'Manage Privileged Accounts' is set to 'Default (Disallow)'.

PAM Access configuration

ADD A PROVIDER

Back to the PAM section, add a provider of any of the 3 types : **Domain User** (AD), **Local User** (SSH) or **SQL User**.

When adding the provider, make sure you keep the **Add Team Folder** and **Add Scan Configuration** options checked.

Provider

GENERAL

Name •

PAM Provider

DOMAIN

Domain name

windjammer.loc

+

User logon type •

Sam Account Name

▼

Protocol •

LDAP

▼

Port

636

CREDENTIALS

i

Make sure you keep a copy of the password, you will not be able to retrieve it later.

Username •

pam_access@windjammer.loc

User Principal Name •

pam_access@windjammer.loc

I

Password

••••••

👁

⋮

Test Connection

ACTIONS

☒ Add Team Folder

☒ Add Scan Configuration

Save

Cancel

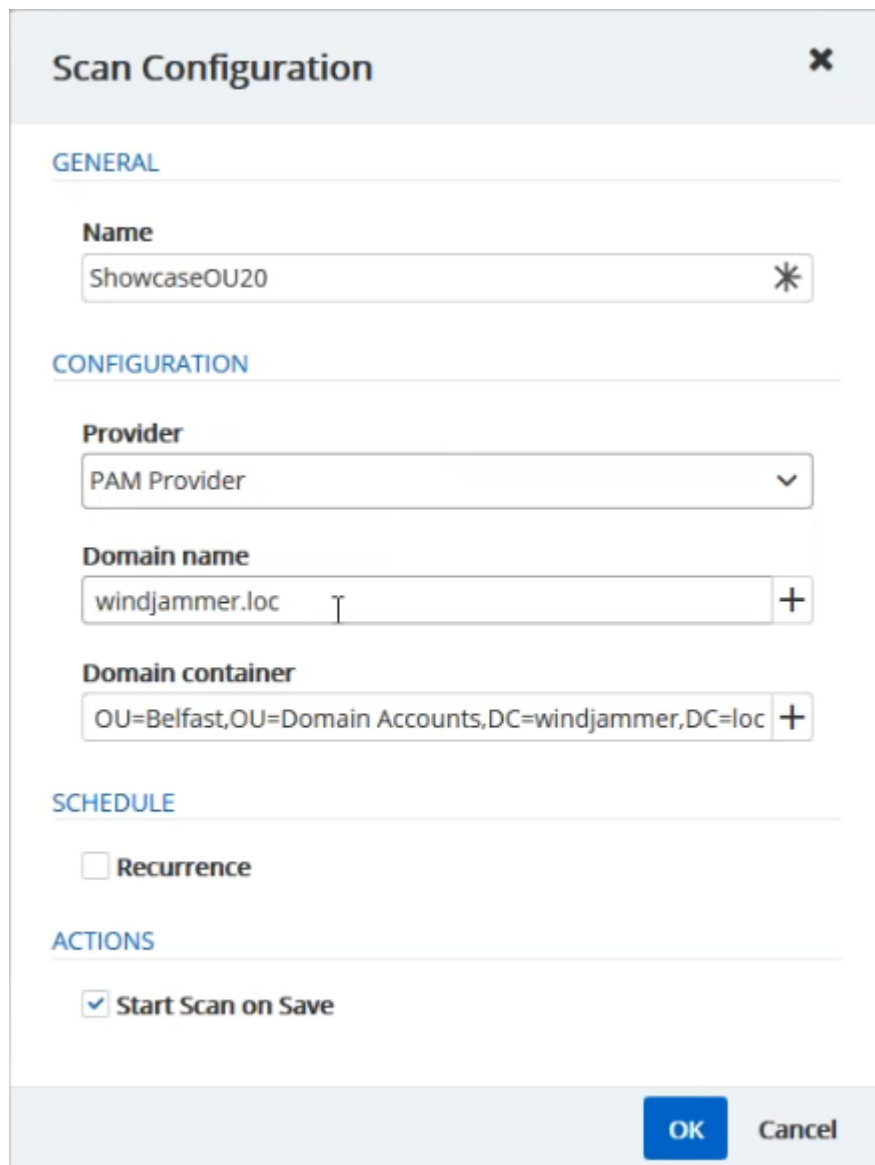
PAM Provider Configuration

© 2020 Devolutions inc.

For more information, please consult the [Providers](#) topic.

ADD A SCAN CONFIGURATION

1. Confirm that it is the good provider, domain and domain container (where the accounts are located).
2. Make sure the **Start Scan on Save** checkbox is selected.
3. Click **OK**.



The image shows a 'Scan Configuration' dialog box with a close button (X) in the top right corner. The dialog is divided into four sections: GENERAL, CONFIGURATION, SCHEDULE, and ACTIONS.

- GENERAL**: Contains a 'Name' field with the text 'ShowcaseOU20' and a '*' icon on the right.
- CONFIGURATION**: Contains three fields:
 - 'Provider': A dropdown menu showing 'PAM Provider' with a downward arrow.
 - 'Domain name': A text field with 'windjammer.loc' and a '+' icon on the right.
 - 'Domain container': A text field with 'OU=Belfast,OU=Domain Accounts,DC=windjammer,DC=loc' and a '+' icon on the right.
- SCHEDULE**: Contains a 'Recurrence' checkbox, which is currently unchecked.
- ACTIONS**: Contains a 'Start Scan on Save' checkbox, which is currently checked.

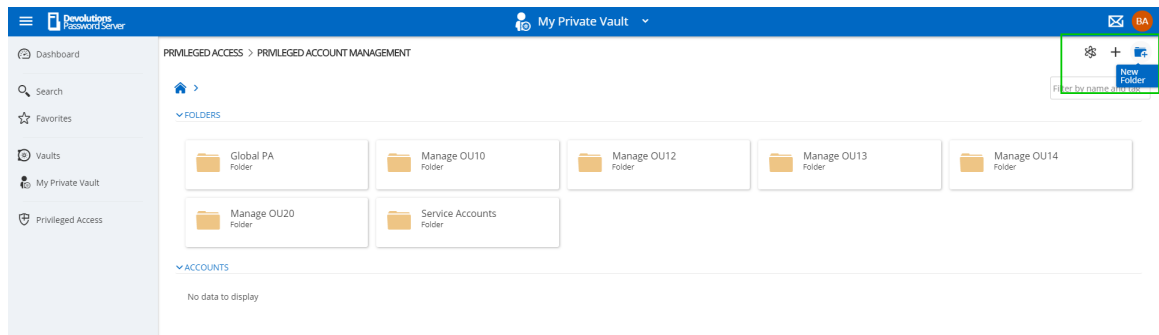
At the bottom right of the dialog are two buttons: 'OK' (in a blue box) and 'Cancel'.

PAM Scan Config

For more information, please refer to the [Scan Configurations](#) topic.

ADD FOLDERS IN THE ACCOUNTS SECTION

In the **Accounts** section of the PAM tab, you need to create a **Folder** to contain the accounts. You can customize that particular [folder's security options](#) if you don't want to give them the defaults you set during the initial configuration. You can also [customize the approvers on the folder](#) directly which will give you a list of the administrators.



PAM Create Folder

IMPORT ACCOUNTS FROM A SCAN

1. In the **Scan Configuration** section, click the result of your initial search.

Status	Name	Scan Type	Last Run Time	Next Run Time	Recurrent	Results	
✓	ShowcaseOU14	Domain	2020-01-20 17:05			3	View Result
✓	ShowcaseOU12	Domain	2020-01-20 16:23			3	View Result
✓	ShowcaseOU20	Domain	2020-01-20 17:10			3	View Result
✓	ShowcaseOU10	Domain	2020-01-20 17:05			3	View Result

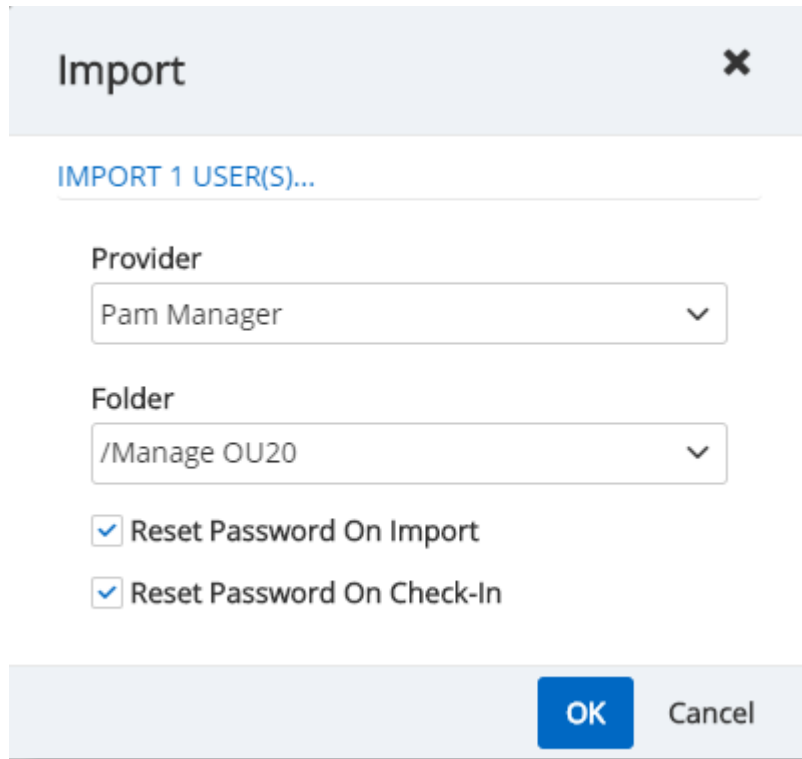
View Scan Results

2. Select all the accounts you want to import, and on the top right, click the **Import** button.

✓	User Principal Name	NetBios Name	SAM Name	First Name	Last Name	Email	Domain
✓	_forestadmin20@windjamme...	WINDJAMMER_forestadmin20	_forestadmin20	Forest	Admin		windjammer.loc
✓	_backupoperator20@windja...	WINDJAMMER_backupoperat...	_backupoperator20	Backup	Operator		windjammer.loc
<input type="checkbox"/>	_financialsmgr20@windjam...	WINDJAMMER_financialsmgr...	_financialsmgr20	Financials	Manager		windjammer.loc

Import Selected Entries

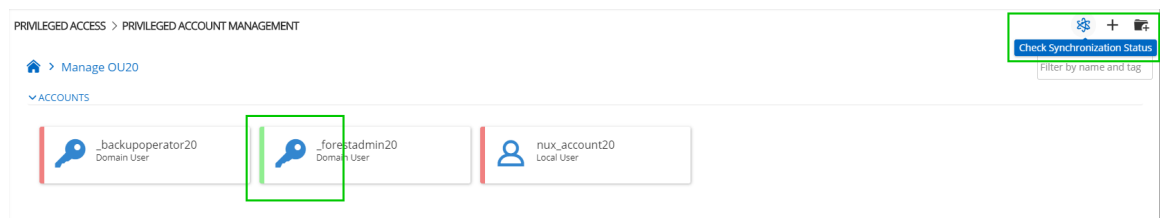
3. You can put them in the folder of your choice. You can also choose whether to reset password on import or on check-in (recommended). That way, the password is safe the moment the user checks it back in.



The image shows a dialog box titled "Import" with a close button (X) in the top right corner. Below the title bar, there is a section labeled "IMPORT 1 USER(S)..." with a horizontal line underneath. The dialog contains two dropdown menus: "Provider" set to "Pam Manager" and "Folder" set to "/Manage OU20". Below these are two checked checkboxes: "Reset Password On Import" and "Reset Password On Check-In". At the bottom right, there are "OK" and "Cancel" buttons.

Import Users

Once imported, you can click into the folder and manually check the **Synchronization Status** in the top right of the screen. You will know the accounts are well synchronized when the credentials have a green bar on the left.



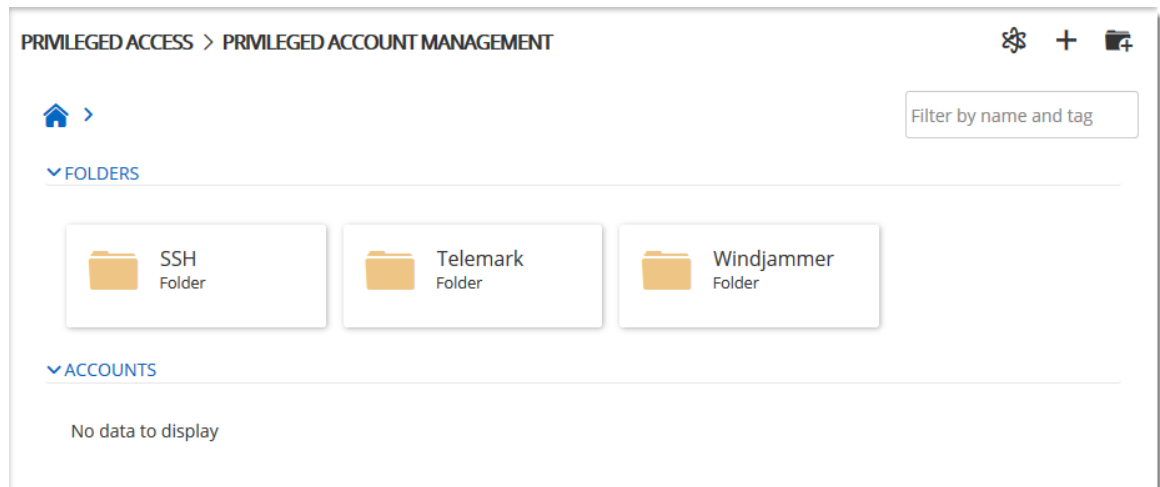
PAM Account Sync Check

You are now ready to use the privileged access management portion of Devolutions Server!

6.2 Accounts

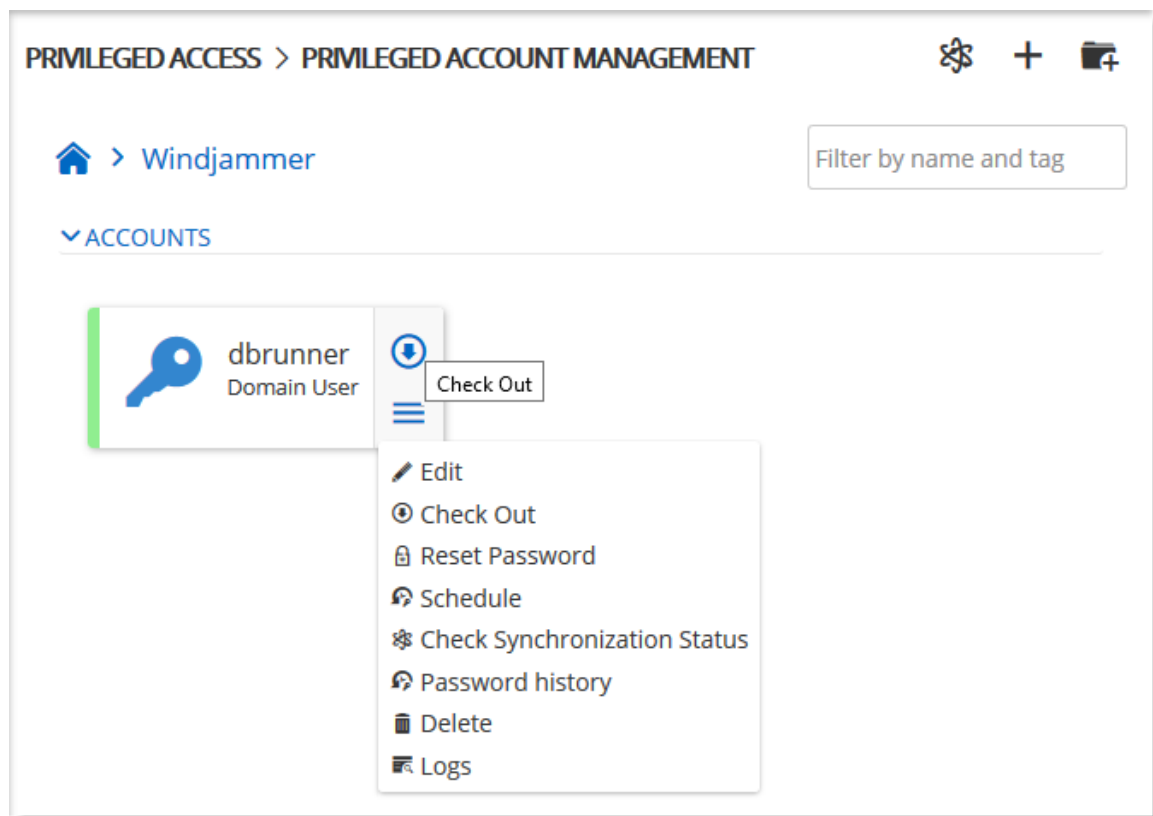
DESCRIPTION

The Accounts section allows to manage all privileged accounts within the Privileged Access Management solution. The accounts can be organized within folders or directly saved in the Root.



Accounts dashboard

For every privileged account, it is possible to manage the checkout/check-in process or to have access to many options described below.



Privileged Accounts folder content

MORE

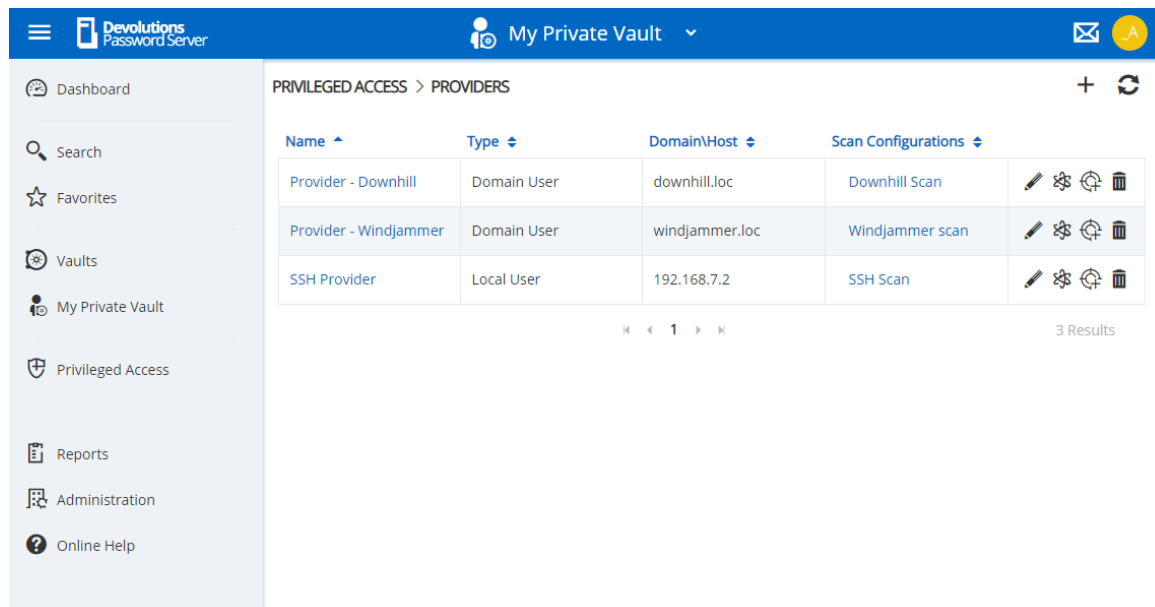
OPTIONS	DESCRIPTION
Edit	Edit the privileged account properties.
Check Out	Access and lock the privileged account.
Reset Password	Reset the password in Devolutions Server and in Active Directory or on the Local SSH machine.
Schedule	Reset the password based on a automated schedule.
Check Synchronization Status	Verify if the Provider can still access the account in the Domain or the Local SSH machine.

OPTIONS	DESCRIPTION
Password history	Open the Password history dialog.
Delete	Remove the account from the Privileged Account Management system without deleting it in the Domain or the Local SSH machine.
Logs	Open the Logs dialog which contains the account's activity.

6.3 Providers

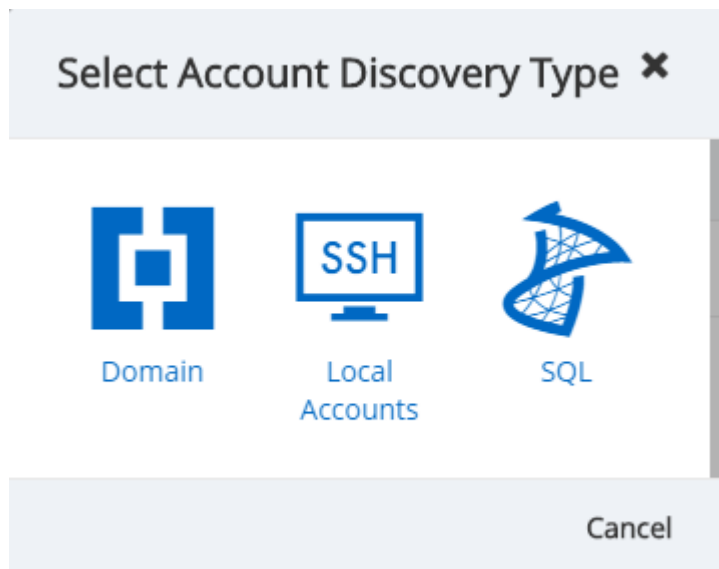
DESCRIPTION

The usage of Providers is required to scan the Active Directory structure, your local network for SSH discovering, and SQL.



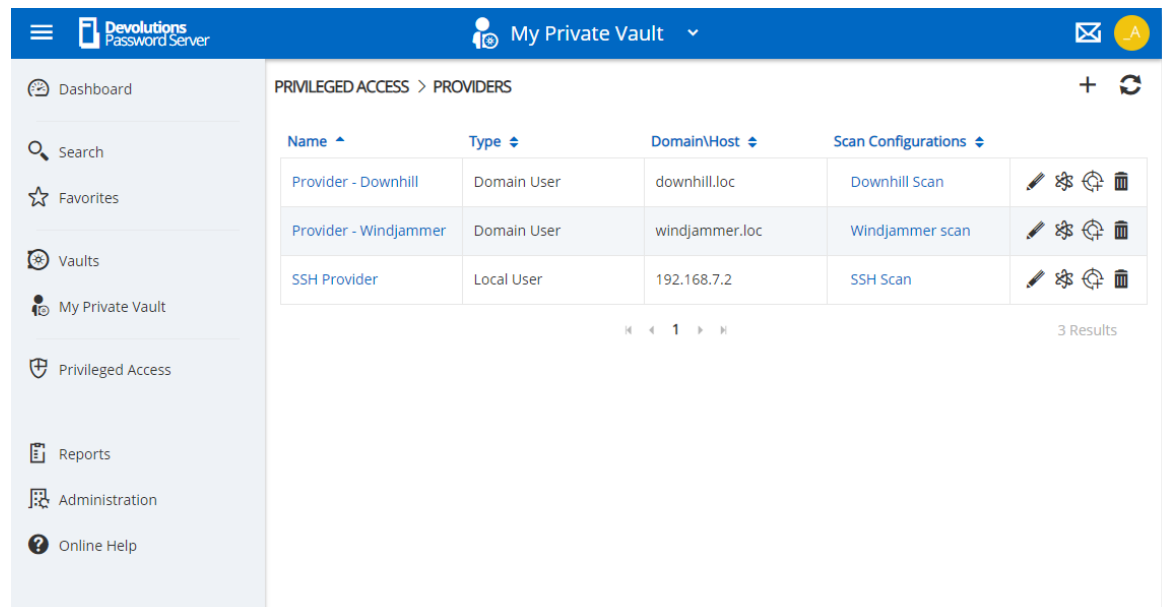
Providers dashboard

On the creation of a Provider, two choices are available: [Domain User](#), [SSH Local User](#), and [SQL User](#). Multiple Providers can be created and can reach different domains as long as the Devolutions Server instance can communicate with the domain controller.



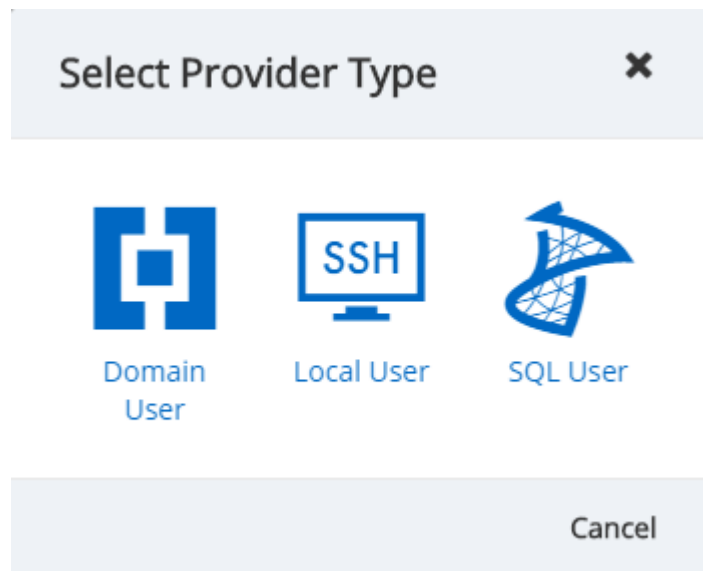
Provider Type dialog

The usage of Providers is required to scan the Active Directory structure, your local network for SSH discovering or your SQL Server accounts.



Providers dashboard

On the creation of a Provider, three choices are available: [Domain User](#), [SQL Server](#) or [SSH Local User](#). Multiple Providers can be created and can reach different domains as long as the Devolutions Server instance can communicate with the domain controller.



Provider Type dialog

6.3.1 Domain Provider

DESCRIPTION

The Domain Provider allows Devolutions Server to store the domain account credentials to be used for Active Directory accounts discovery or to achieve password rotation.

Provider

GENERAL

Name •
Provider - Windjammer

DOMAIN

Domain name
windjammer.loc

Protocol • LDAP
Port

CREDENTIALS

i Make sure you keep a copy of the password, you will not be able to retrieve it later.

Username •
administrator@windjammer.loc

Password
.....

Save **Cancel**

Domain Provider dialog

GENERAL

OPTIONS	DESCRIPTION
Name	Display name of the Provider.

DOMAIN

OPTIONS	DESCRIPTION
Domain name	FQDN of the domain against where the scan or the password rotation will be executed.
Protocol	Protocol used to contact the domain controller. Select between: <ul style="list-style-type: none">• LDAP• LDAPS
Port	Set the port number used with the configured Protocol.

CREDENTIALS

OPTIONS	DESCRIPTION
Username	Username of the domain account.
Password	Password of the domain account.

6.3.2 Local SSH Provider

DESCRIPTION

The SSH Provider allows Devolutions Server to store the SSH local account credentials to be used for SSH accounts discovery or to achieve password rotation.

Provider

GENERAL

Name

SSH Provider

HOST

Host

192.168.7.2

Port

22

CREDENTIALS

Make sure you keep a copy of the password, you will not be able to retrieve it later.

Username

MyUsername

Password

.....

Test Connection

Save

Cancel

SSH Provider dialog

GENERAL

© 2020 Devolutions inc.

OPTIONS	DESCRIPTION
Name	Display name of the Provider.

HOST

OPTIONS	DESCRIPTION
Host	IP Address or host name where the SSH accounts are located.
Port	Set the port number used to communicate with the host.

CREDENTIALS

OPTIONS	DESCRIPTION
Username	Username of the SSH account.
Password	Password of the SSH account.

6.3.3 SQL Server Provider

DESCRIPTION

The SQL Provider allows Devolutions Server to store the SQL account credentials to be used for SQL accounts discovery or to achieve password rotation.

Provider

GENERAL

Name •

SQL Provider

SERVER

Server name •

.....

windjammer.loc\SQL2016

Advanced

CREDENTIALS

i

Make sure you keep a copy of the password, you will not be able to retrieve it later.

Username •

sa

Password

.....

👁

⋮

Test Connection

Save

Cancel

SQL Provider dialog

GENERAL

OPTIONS	DESCRIPTION
Name	Display name of the Provider.

© 2020 Devolutions inc.

SERVER

OPTIONS	DESCRIPTION
Server	Hostname of the SQL Server

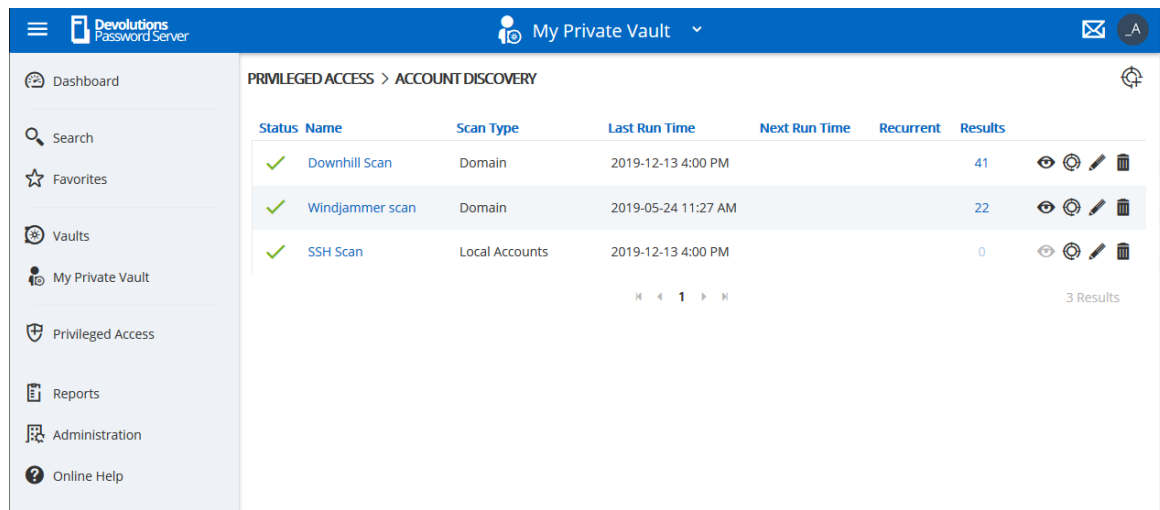
CREDENTIALS

OPTIONS	DESCRIPTION
Username	Username of the SQL account with rights to list accounts.
Password	Password of the SQL account.

6.4 Scan Configurations

DESCRIPTION

The Scan Configurations or Account Discovery is the configured instance that will discover accounts in a domain, a SQL server or SSH environment.



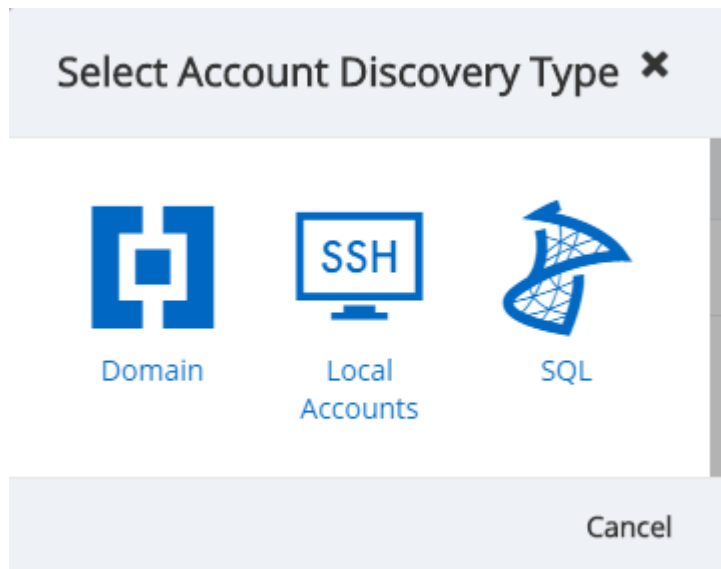
The screenshot shows the Devolutions Password Server interface. The left sidebar contains navigation links: Dashboard, Search, Favorites, Vaults, My Private Vault, Privileged Access, Reports, Administration, and Online Help. The main content area is titled 'PRIVILEGED ACCESS > ACCOUNT DISCOVERY'. It displays a table with the following data:

Status	Name	Scan Type	Last Run Time	Next Run Time	Recurrent	Results	
✓	Downhill Scan	Domain	2019-12-13 4:00 PM			41	👁️ ⚙️ ✎️ 🗑️
✓	Windjammer scan	Domain	2019-05-24 11:27 AM			22	👁️ ⚙️ ✎️ 🗑️
✓	SSH Scan	Local Accounts	2019-12-13 4:00 PM			0	👁️ ⚙️ ✎️ 🗑️

At the bottom of the table, there is a pagination control showing '1' and '3 Results'.

Account Discovery dialog

On the creation of an Account Discovery, it is possible to choose between [Domain](#), [SQL Server](#) or [SSH Local Accounts](#).

*Account Type Options*

To see the results of the discovery process, click on the eye icon of the Account Discovery to see the list of accounts.

	User Principal Name	NetBios Name	SAM Name	First Name	Last Name	Email	Domain
<input type="checkbox"/>	dbrunner2@down...	DOWNHILL\dbrun...	dbrunner2	DBRunner2			downhill.loc
<input type="checkbox"/>	pedro@downhill.loc	DOWNHILL\pedro	pedro	Pedro			downhill.loc
<input type="checkbox"/>	roaming@downhill...	DOWNHILL\roami...	roaming	Roaming user			downhill.loc
<input type="checkbox"/>	duo@downhill.loc	DOWNHILL\duo	duo	Duo			downhill.loc
<input type="checkbox"/>	downtest@downh...	DOWNHILL\downt...	downtest	downtest			downhill.loc
<input type="checkbox"/>	DisableMeTest@d...	DOWNHILL\Disabl...	DisableMeTest	DisableMe	Test		downhill.loc
<input type="checkbox"/>	test@downhill.loc	DOWNHILL\test	test	test			downhill.loc
<input type="checkbox"/>	testhubert@down...	DOWNHILL\testhu...	testhubert	Hubert			downhill.loc
<input type="checkbox"/>	test1@downhill.loc	DOWNHILL\test1	test1	test1		test1@downhill.co...	downhill.loc
<input type="checkbox"/>	aroy@downhill.loc	DOWNHILL\aroy	aroy	Alexandre	Roy		downhill.loc

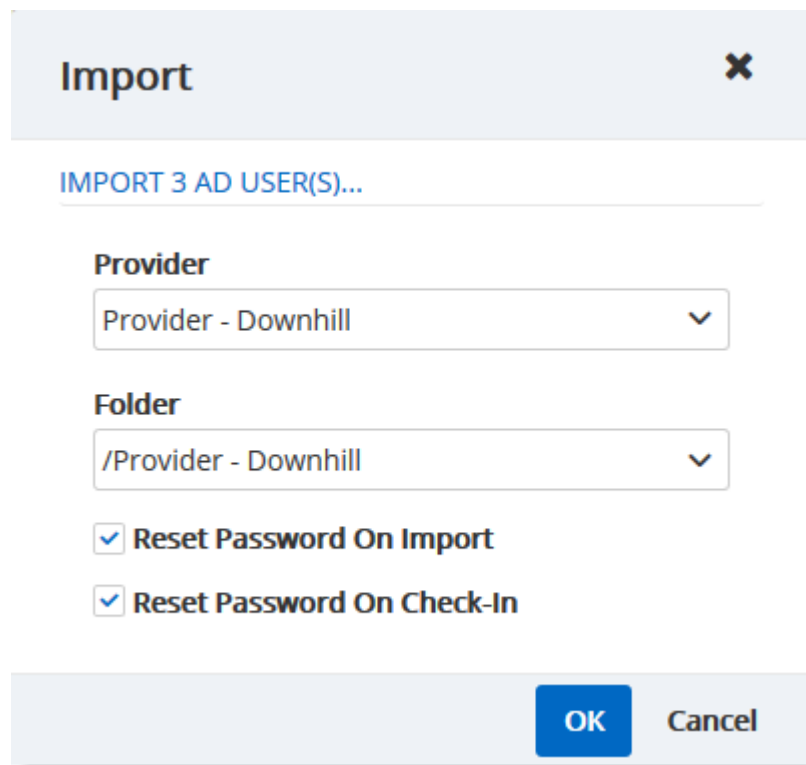
Account Discovery results dialog

In order to manage privileged accounts with the Devolutions Server PAM feature, select the accounts from the Account Discovery results page and click on the Import Selected Accounts button. Then the accounts will be available in Privileged Access - Accounts.

	User Principal Name	NetBios Name	SAM Name	First Name	Last Name	Email	Domain
<input checked="" type="checkbox"/>	walter@downhillp...	DOWNHILL\walter	walter	Walter	Harp		downhill
<input checked="" type="checkbox"/>	TestE@downhill.loc	DOWNHILL\TestE	TestE	TestQ			downhill.loc
<input checked="" type="checkbox"/>	Hpotter@downhill...	DOWNHILL\Hpotter	Hpotter	Harry	Potter		downhill.loc

Import Selected Accounts operation

On import, the [Provider](#), Destination Folder and Reset Password options can be set.



The image shows a dialog box titled "Import" with a close button (X) in the top right corner. Below the title bar, there is a text field containing "IMPORT 3 AD USER(S)...". Underneath, there are two dropdown menus: "Provider" with the selected value "Provider - Downhill" and "Folder" with the selected value "/Provider - Downhill". Below these are two checked checkboxes: "Reset Password On Import" and "Reset Password On Check-In". At the bottom right, there are two buttons: "OK" (in a blue box) and "Cancel".

Import Window

IMPORT

OPTIONS	DESCRIPTION
Provider	Select the Provider in the drop-down list.
Folder	Select the destination folder in the drop-down list.
Reset Password On Import	On import, the password will be reset.
Reset Password On Check-In	When the user will release the account on Check-In, the password will be reset.

6.4.1 Domain Account Discovery

DESCRIPTION

The Domain Account Discovery allows Devolutions Server to scan a domain area to find accounts. The accounts will not be automatically added.

Scan Configuration

GENERAL

Name

Windjammer scan

CONFIGURATION

Provider

Provider - Windjammer

Domain name

windjammer.loc

Domain container

SCHEDULE

☒ Recurrence

Start

05/24/2019 07:26

Every

1

Unit

Minutes

Hours

Days

ACTIONS

☐ Start Scan on Save

OK

Cancel

Domain Account Discovery dialog

© 2020 Devolutions inc.

GENERAL

OPTIONS	DESCRIPTION
Name	Display name of the Domain Account Discovery.

CONFIGURATION

OPTIONS	DESCRIPTION
Provider	Name of the Domain Provider.
Domain name	FQDN of the domain against where the scan or the password rotation will be executed.
Domain Container	Distinguished name of an Active Directory OU or group.

SCHEDULE

OPTIONS	DESCRIPTION
Recurrence	If enable, will run the Account Discovery on a regular basis depending on the schedule configuration.
Start	Starting date and hour of the Account Discovery recurrence.
Every	Number of Units.
Unit	Units of time.

ACTION

OPTIONS	DESCRIPTION
Start Scan on Save	If enabled, will start the account discovery scan on saving the modifications.

6.4.2 SSH Account Discovery

DESCRIPTION

The SSH Account Discovery allows Devolutions Server to scan the host to find accounts. The accounts will not be automatically added.

Scan Configuration

GENERAL

Name

SSH Scan*

CONFIGURATION

Provider

SSH Provider

Host

192.168.7.2

SCHEDULE

☒ Recurrence

Start

12/13/2019 11:28

Every

1

Unit

Minutes

Hours

Days

ACTIONS

☐ Start Scan on Save

OK

Cancel

SSH Account Discovery dialog

GENERAL

© 2020 Devolutions inc.

OPTIONS	DESCRIPTION
Name	Display name of the SSH Account Discovery.

CONFIGURATION

OPTIONS	DESCRIPTION
Provider	Name of the SSH Provider.
Host	IP of the host where the scan or the password rotation will be executed.

SCHEDULE

OPTIONS	DESCRIPTION
Recurrence	If enable, will run the Account Discovery on a regular basis depending on the schedule configuration.
Start	Starting date and hour of the Account Discovery recurrence.
Every	Number of Units.
Unit	Units of time.

ACTION

OPTIONS	DESCRIPTION
Start Scan on Save	If enabled, will start the account discovery scan on saving the modifications.

6.4.3 SQL Account Discovery

DESCRIPTION

The SQL Account Discovery allows Devolutions Server to scan the host to find accounts. The accounts will not be automatically added.

Scan Configuration

GENERAL

Name

SQL Scan config

CONFIGURATION

Provider

SQL Provider

Database name

SCHEDULE

☐ Recurrence

ACTIONS

☒ Start Scan on Save

OK

Cancel

SQL Account Discovery dialog

GENERAL

OPTIONS	DESCRIPTION
Name	Display name of the SQL Account Discovery.

CONFIGURATION

OPTIONS	DESCRIPTION
Provider	Name of the SQL Provider.
Database Name	Name of the Database, the scan will list the accounts in that database

SCHEDULE

OPTIONS	DESCRIPTION
Recurrence	If enable, will run the Account Discovery on a regular basis depending on the schedule configuration.
Start	Starting date and hour of the Account Discovery recurrence.
Every	Number of Units.
Unit	Units of time.

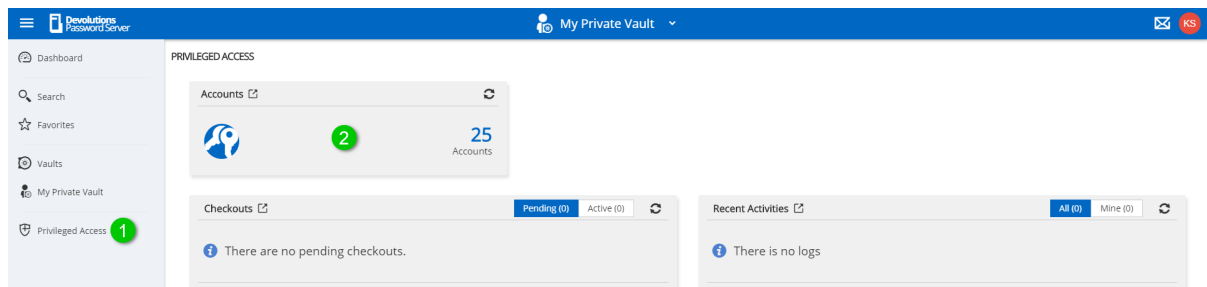
ACTION

OPTIONS	DESCRIPTION
Start Scan on Save	If enabled, will start the account discovery scan on saving the modifications.

6.5 Checkout Process

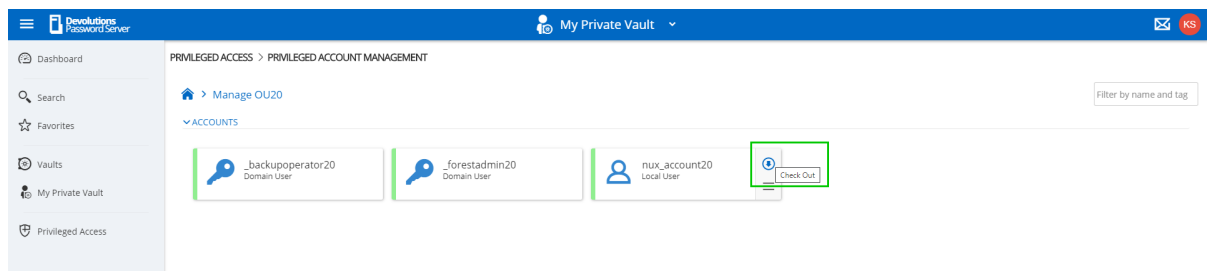
DESCRIPTION

1. To check out an entry requiring approbation, the user needs to go to the **Privileged Access** section on the Devolutions Server's webpage.
2. The user then clicks on the **Accounts** panel.



Privileged Access

The user then locates the account they want to check out for temporary use and clicks the **Check Out** button on the entry.



PAM Account Selection

A pop-up will appear requesting information on the checkout request to be sent to an administrator for approval.

Check Out - Request

Reason (Optional)

I need to checkout this account to access a secure server. Please approve.

Duration (in minutes)

60

Approver

Bob Anderson

Request checkout

Close

Checkout Request

Once the request is sent, the selected Approver will have the request in the **Checkout** field of his **Privileged Access** window.

Devolutions
Password server

WD Windjammer Defa...

BA

Dashboard

Search

Favorites

Vaults

My Private Vault

Privileged Access

PRIVILEGED ACCESS

Accounts 25 Accounts

Providers 2 Providers

Scan Configurations 6 Scan Configurations

Checkouts Pending (1) Active (0)

Kelly Slater Requested By

2020-03-04 14:27

nux_account20

Approver: Bob Anderson

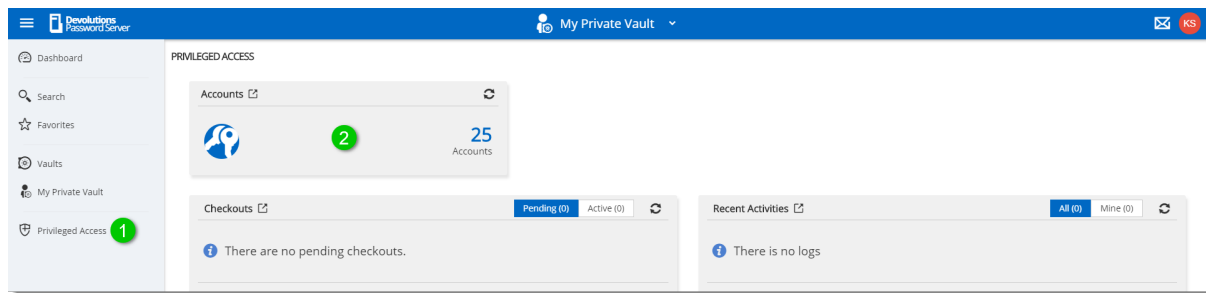
Recent Activities

All (0) Mine (0)

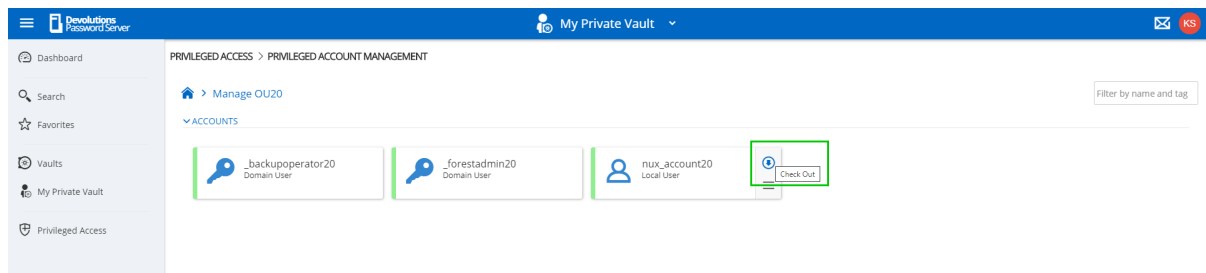
There is no logs

Checkout Request

1. To check out an entry requiring approbation, the user needs to go to the Privileged Access section on the Devolutions Server's webpage.
2. The user then clicks on the Accounts panel.

*Privileged Access*

The user then locates the account they want to Check Out for temporary use and clicks the **Check Out** button on the entry.

*PAM Account Selection*

A pop-up will appear requesting information on the checkout request to be sent to an administrator for approval.

Check Out - Request

Reason (Optional)

I need to checkout this account to access a secure server. Please approve.

Duration (in minutes)

60

Approver

Bob Anderson

Request checkout

Close

Checkout Request

Once the request is sent, the selected Approver will have the request in the "Checkout" field of his **Privileged Access** window.

Devolutions Password Server

WD Windjammer Defa...

BA

Dashboard

Search

Favorites

Vaults

My Private Vault

Privileged Access

PRIVILEGED ACCESS

Accounts 25 Accounts

Providers 2 Providers

Scan Configurations 6 Scan Configurations

Checkouts Pending (1) Active (0)

Kelly Slater Requested By

2020-03-04 14:27

nux_account20

Approver: Bob Anderson

Recent Activities

All (0) Mine (0)

There is no logs

Checkout Request

The approver gets the following pop-up when clicking on the request where it's possible to either **Approve** or **Deny** the request and leave an optional message.

Checkout request: nux_account20 - Status: Pending

Checkout Owner

Kelly Slater

Requested Approver

Bob Anderson

Checkout Reason

I need to checkout this account to access a secure server. Please approve.

Duration (in minutes)

60

Approver Message

Approve

Deny

Close

Approve/Deny Window

If the request is denied, the user will see that their request on the account is no longer pending and was denied in the recent activity field of the main **Privileged Access** page. If approved, they will be able to access the account by clicking on the same button they used to submit the request. They'll now get this **Active Checkout** window instead of the request one :



Checkout Active

Once done with the account, they can use the **CheckIn** button on the last window to release their hold on the checkout.

Privileged accounts' passwords are automatically changed on check-in if the corresponding option is enabled.

6.6 View Sensitive Data vs Account Brokering

DESCRIPTION

It is important to learn the differences between the 2 sets of permissions known as **View sensitive data on checkout** and **Credential Brokering**. In this topic, you will find an explanation of the way they're used.

Giving access to **View Sensitive Data on Checkout** to a user will let that user see the password when the entry is checked out.

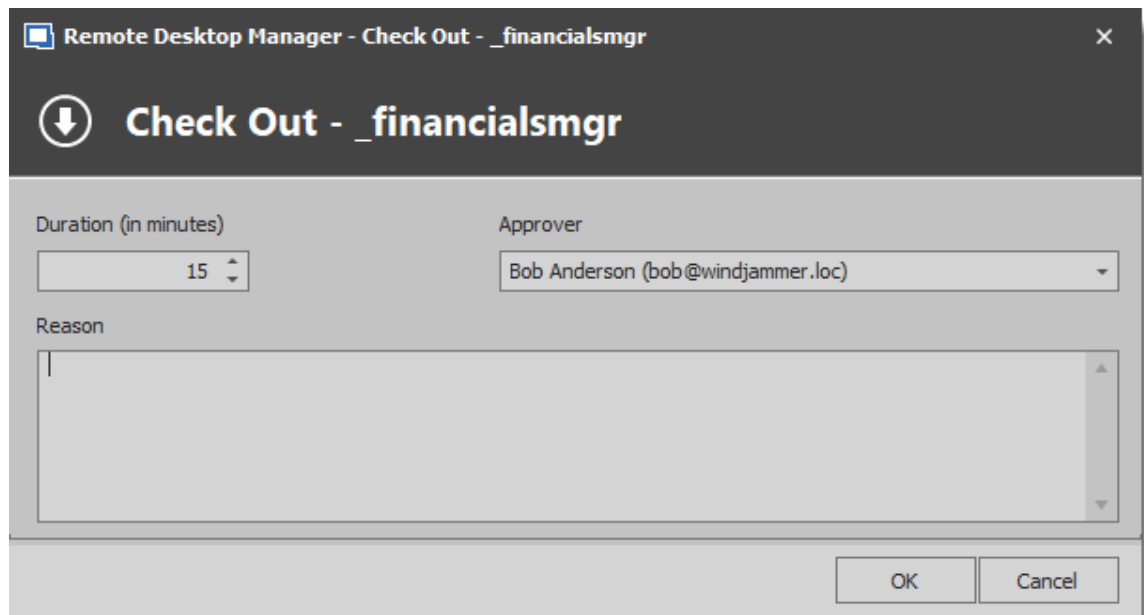
The screenshot shows a window titled "Check Out - Active" with a timer at 00:05:41. Below the title bar is a text input field containing the alphanumeric string "UEAfzES!e59c!jUo^PT3". To the right of the input field is a green-bordered box containing two icons: a document with a checkmark and an eye. At the bottom right of the window are two buttons: "Checkin" (in blue) and "Close".

With Access

The screenshot shows a window titled "Check Out - Active" with a timer at 00:05:53. Below the title bar is a text input field containing six dots "*****". To the right of the input field is a green-bordered box containing a single empty input field. At the bottom right of the window are two buttons: "Checkin" (in blue) and "Close".

Without access

Credential Brokering lets a user check out credentials for a session from Remote Desktop Manager directly on the entry itself. When opening the session that requires a privileged account, a pop-up can appear with the **checkout request** window if the entry requires approval. Following the approval, the user will be able to launch the session successfully. Otherwise, the entry will be used seamlessly to open the session.



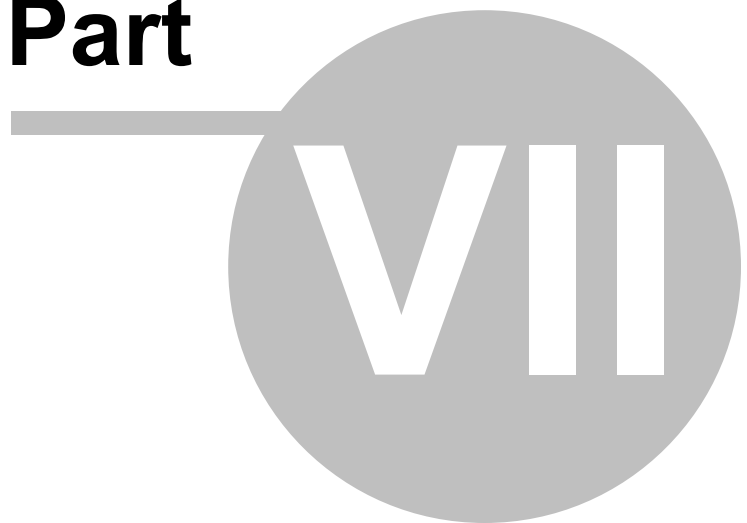
The screenshot shows a dialog box titled "Remote Desktop Manager - Check Out - _financialsmgr". The main heading is "Check Out - _financialsmgr" with a download icon. The dialog contains three fields: "Duration (in minutes)" with a value of 15, "Approver" with a dropdown menu showing "Bob Anderson (bob@windjammer.loc)", and a "Reason" text area. At the bottom right are "OK" and "Cancel" buttons.

Field	Value
Duration (in minutes)	15
Approver	Bob Anderson (bob@windjammer.loc)
Reason	

Credential Brokering Checkout Request

Devolutions Web Login

Part



7 Devolutions Web Login




7.1 Overview

DESCRIPTION



Devolutions Web Login is a web browser password plugin used in conjunction with Remote Desktop Manager, Devolutions Password Server and Devolutions Password Hub, which allows users to securely inject passwords into websites using credentials stored in their vaults.

It gives system administrators full control over the management of passwords, without affecting the user's productivity.

 <p>Remote Desktop Manager</p> <p>Centralize, Manage and Secure Remote Connections</p>	 <p>Devolutions Password Server</p> <p>Secure, Manage and Monitor Access to Privileged Accounts</p>	 <p>Devolutions Password Hub</p> <p>Vault and Manage Business-User Passwords</p>
<p>Remote Desktop Manager centralizes all remote connections on a single platform that is securely shared between users and across the entire team.</p>	<p>Devolutions Password Server lets you control access to privileged accounts and manage remote sessions through a secure solution that can be deployed on-premises.</p>	<p>Devolutions Password Hub is a secure and cloud-based password manager for teams</p>



Advanced users, other browser extensions, or even JavaScript injection can all result in the password being read from the password edit control, even if it displays dots instead of the password. Any use of an external browser must be carefully weighed against your security requirements.



Warning for all Remote Desktop Manager users:

Devolutions Web Login was created for a normal desktop environment. It uses inter process communication (IPC) with the client application. Using it on a terminal server introduces a level of risk that may be unacceptable for corporate users.

To use it in a safe manner, it is critical that each user is assigned a distinct port and that port be kept secret. An application passcode must be set as well to secure the port. The first client application that starts will be able to use the port exclusively. All **Devolutions Web Login** calling on that port **will get the responses**, unless an application passcode is required.

7.2 Installation

DESCRIPTION

Devolutions Web Login is a free browser extension companion tools. It does require one of our products to function at this time.

Click on the browser link below to start the installation of Devolutions Web Login plugin:

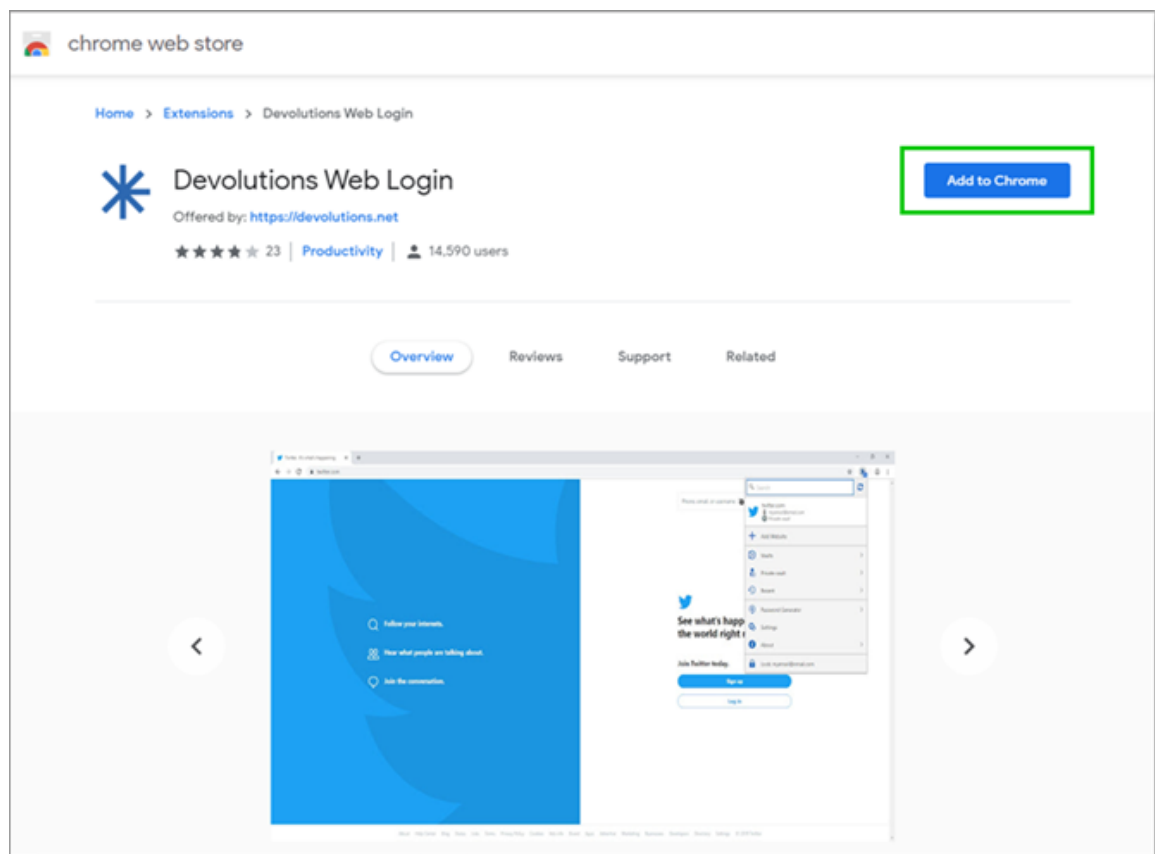
- [Chrome](#)
- [Firefox](#)
- [Microsoft Edge](#)
- [Opera](#)

7.2.1 Chrome

DESCRIPTION

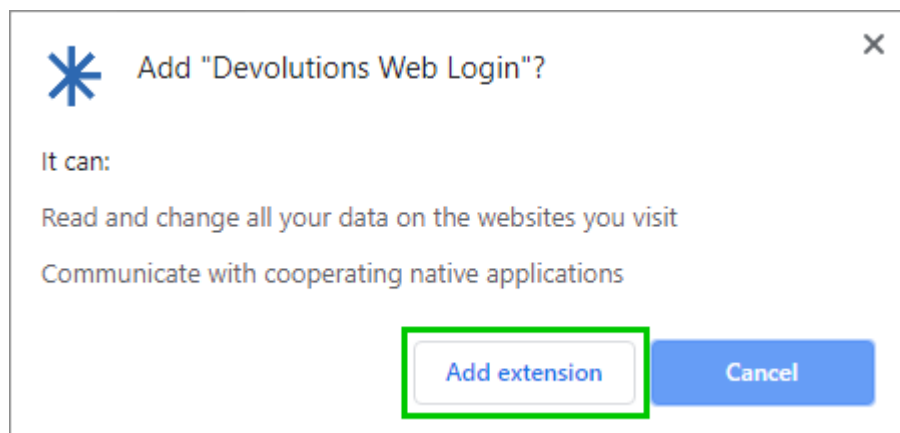
Follow the steps below to complete the installation of Devolutions Web Login in the Google Chrome web browser.

1. Open Google Chrome.
2. Navigate to [Devolutions Web Login extension](#) or use the link from our [Website](#)
3. Click the **Add To Chrome** button.



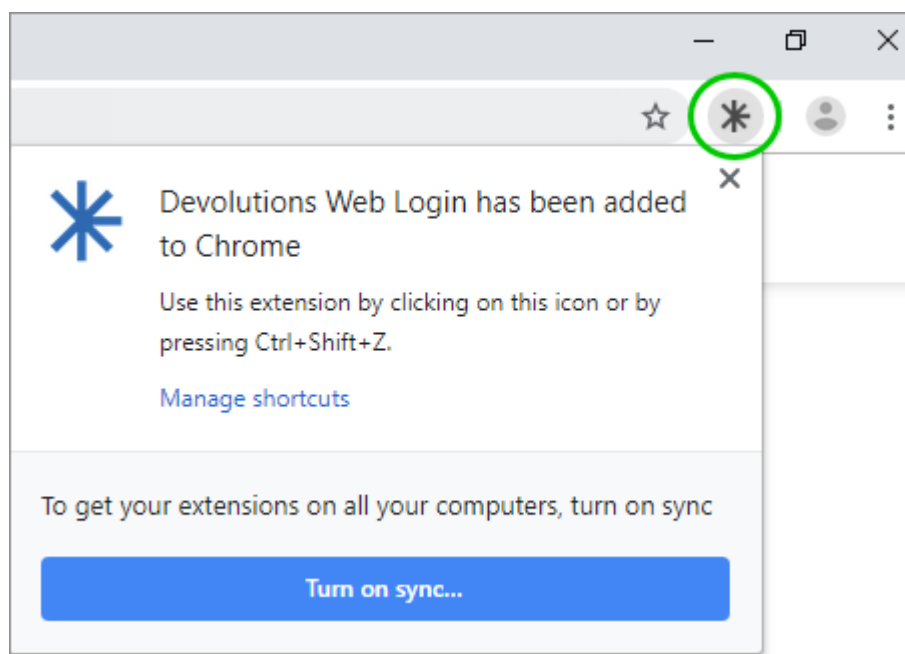
Devolutions Web Login Chrome Web Store

4. Click **Add extension** in the confirmation dialog.



Extension Installation Confirmation

Once installed, access the extension by clicking * in the top-right corner of the Google Chrome web browser.



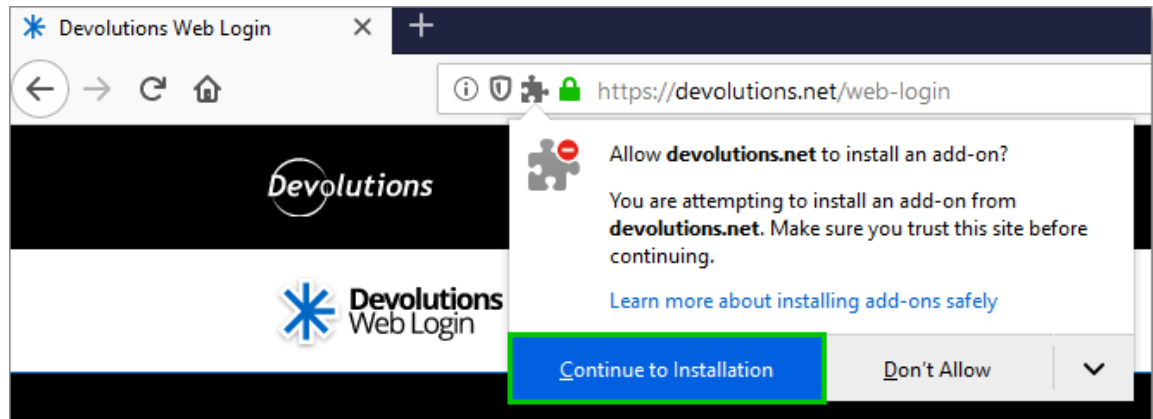
Devolutions Web Login Extension Button

7.2.2 Firefox

DESCRIPTION

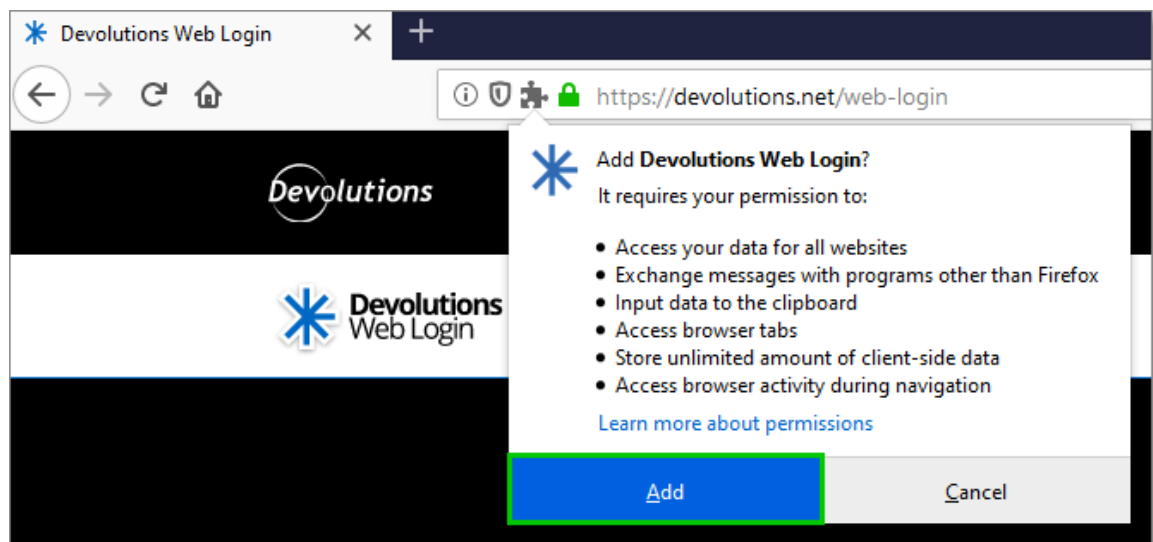
Follow the steps below to complete the installation of Devolutions Web Login in the Firefox web browser.

1. Open a Firefox window.
2. Download the extension from our [Devolutions Web Login](https://devolutions.net/web-login) website page.
3. Click **Continue to Installation** in the confirmation dialog.



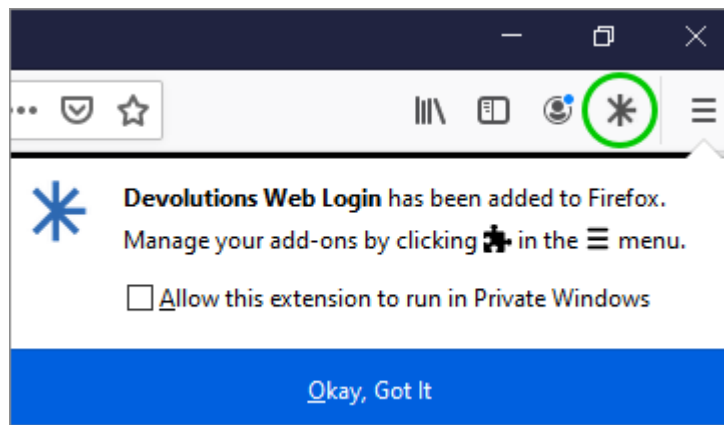
Continue to Installation

4. Click **Add**, when prompted to add Devolutions Web Login to the extension.



Add the Extension

5. Once installed, access the extension by clicking * in the top-right corner of Firefox.



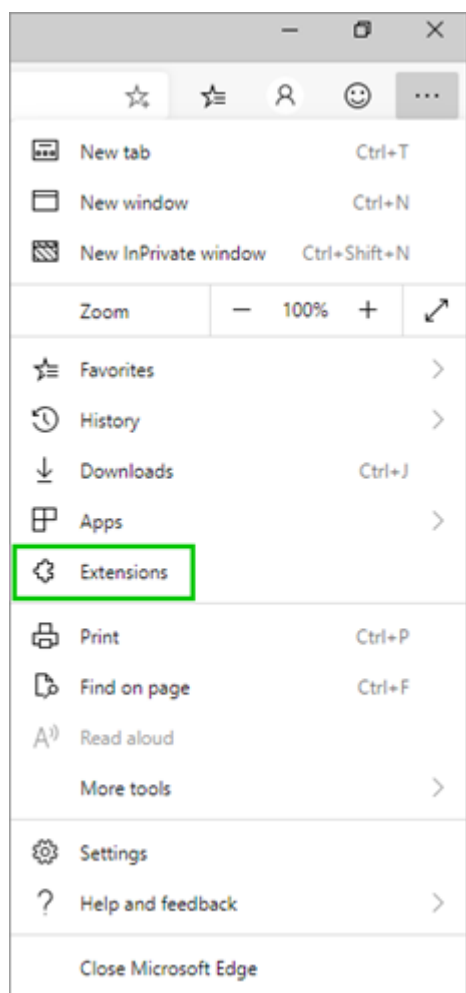
Devolutions Web Login Extension Button

7.2.3 Microsoft Edge Beta

DESCRIPTION

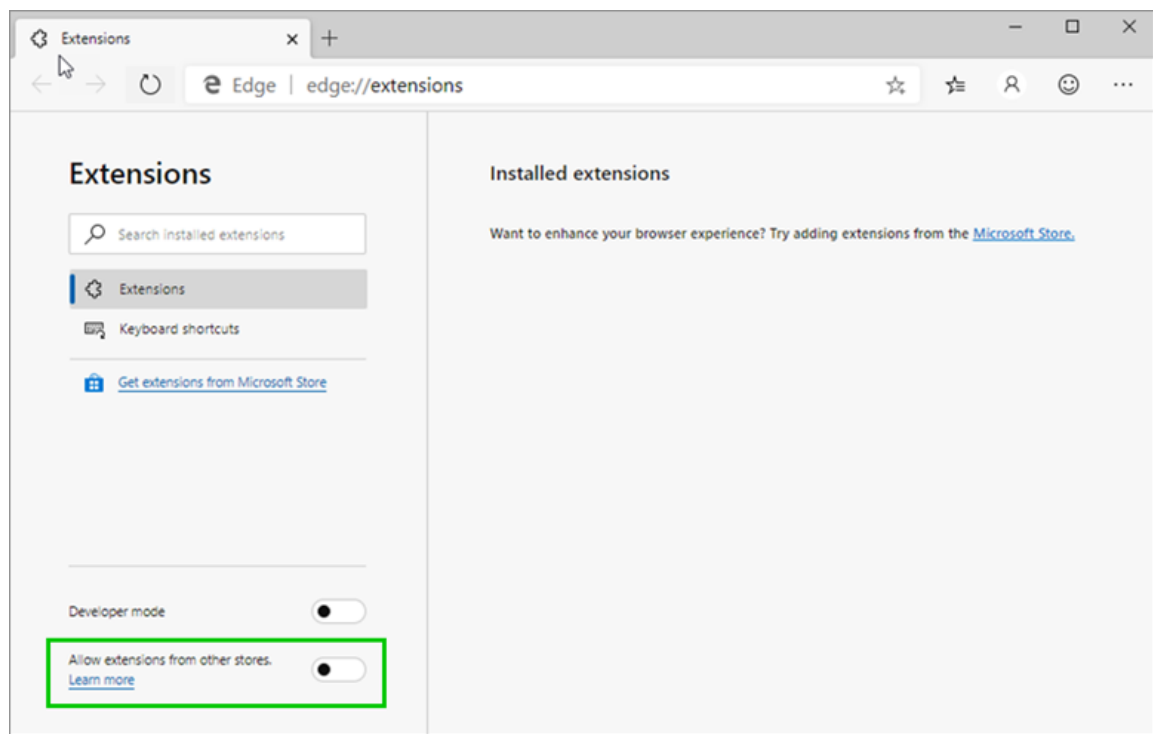
Here are the steps to install Devolutions Web Login on Microsoft Edge Beta.

1. Open [Microsoft Edge Beta](#).
2. Click on **Extensions** in the menu of the browser.



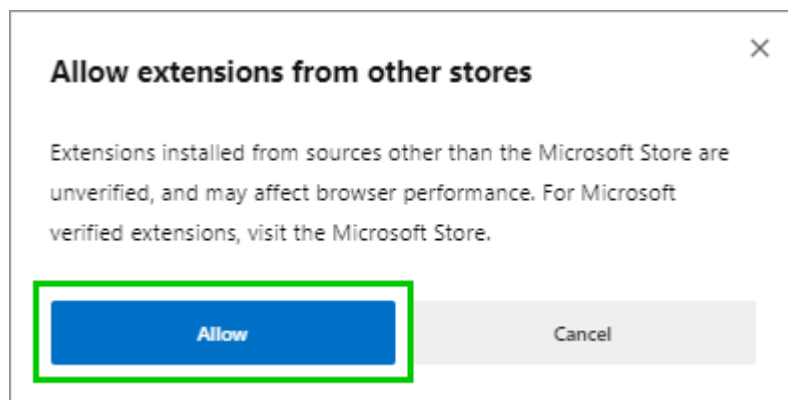
Microsoft Edge Beta Menu

3. Allow extensions from other stores.



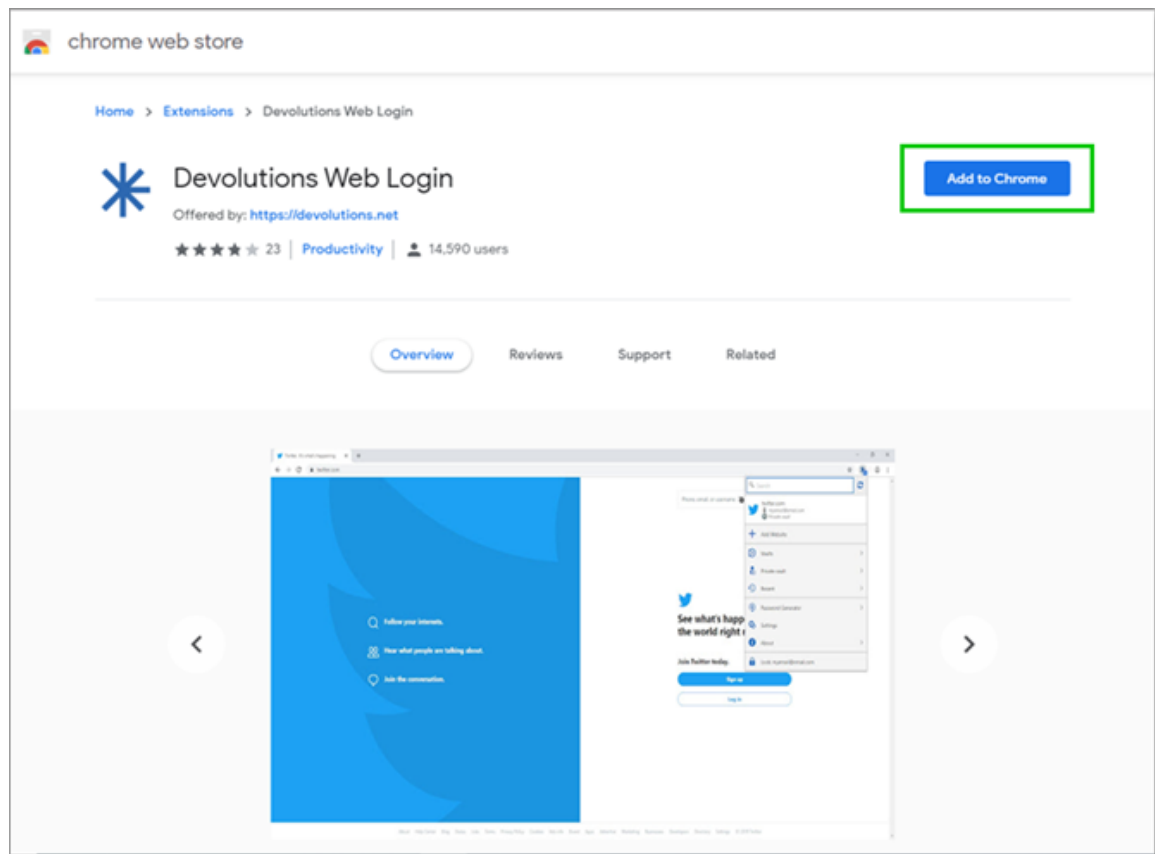
Allow Extensions

4. Allow Non Microsoft Store Extensions.



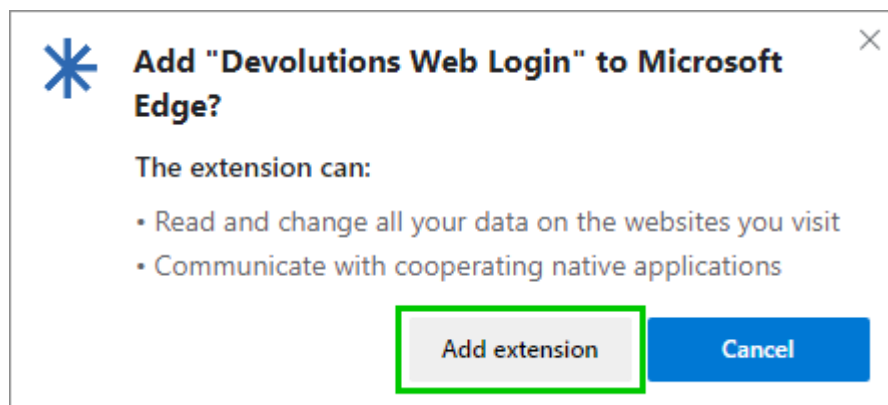
Allow Non Microsoft Store Extensions

5. Follow the extension from [Devolutions Web Login](#) website page to the Chrome Web Store.
6. Click **Add to Chrome**.



Chrome Web Store

7. Add the extension to Microsoft Edge Beta.



Add Devolutions Web Login to Microsoft Edge Beta

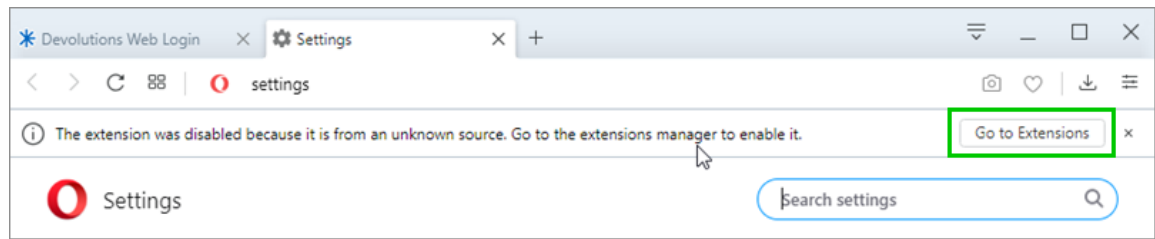
The extension is installed. Access it by clicking * in the top-right corner of the Microsoft Edge Beta web browser.

7.2.4 Opera

DESCRIPTION

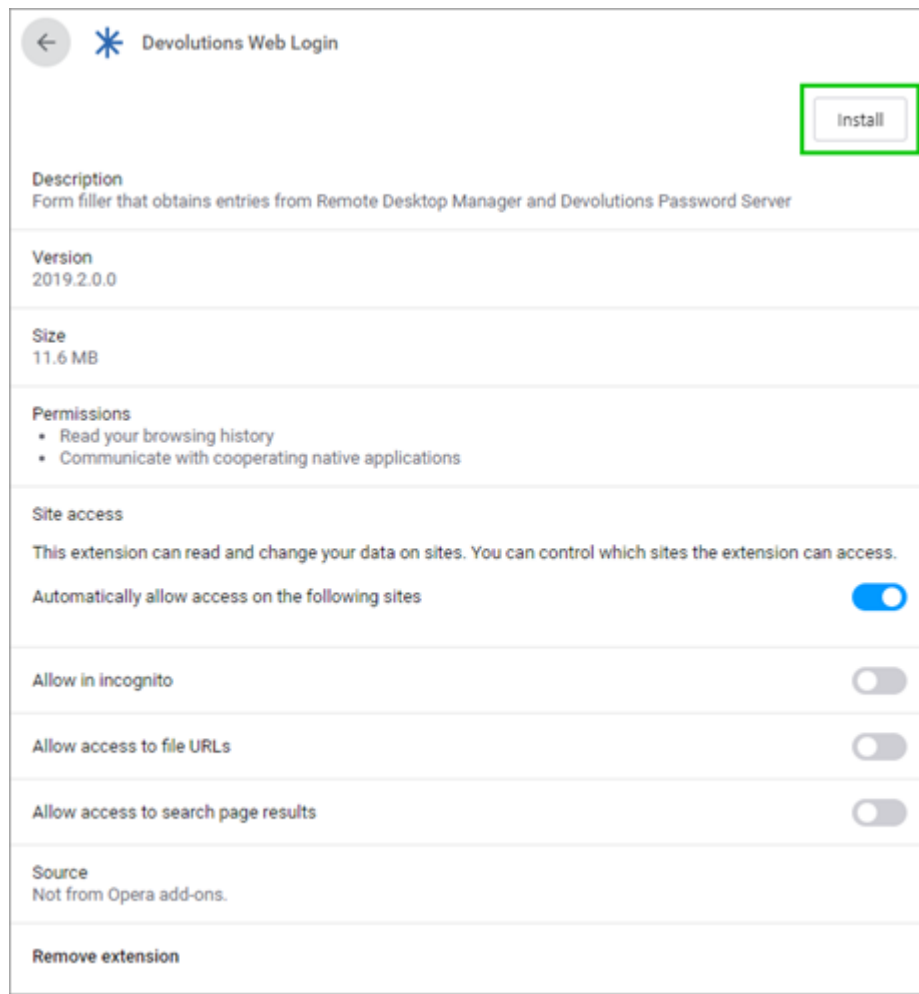
Follow the steps below to complete the installation of Devolutions Web Login in the Opera web browser.

1. Open Opera.
2. Download the extension of [Devolutions Web Login](#) from our website page.
3. Go to **Browser Settings** in the easy setup of Opera.
4. Drag and drop the .nex file from step 2 from the downloads in the web browser.
5. Click on **Go to Extension** from the information panel at the top.



Opera Extensions Enabling

6. Click **Install** and the **Yes, install** pop up.



Opera Install Window

7. Access the extension by clicking * in the top-right corner of Opera.

7.3 First Login

7.3.1 Password Hub

DESCRIPTION

FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

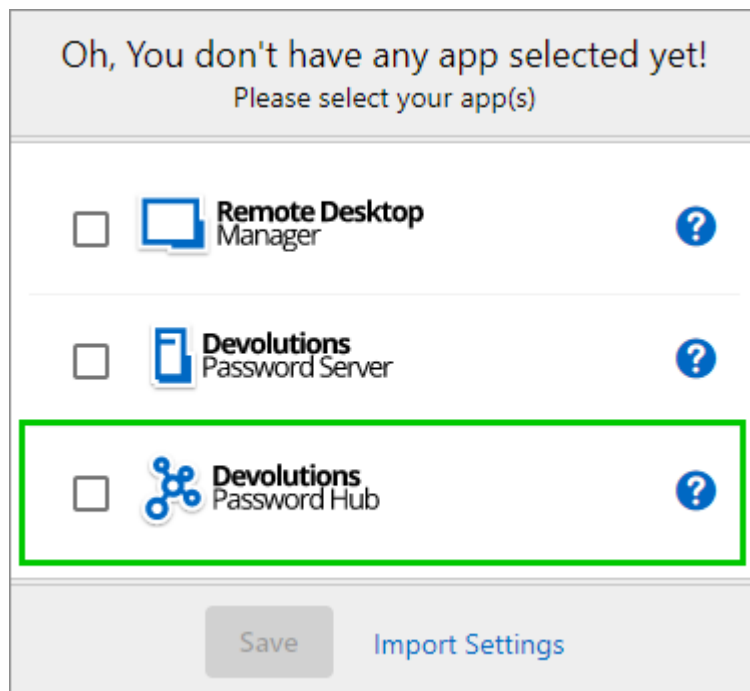
Follow these steps to connect Devolutions Password Hub to Devolutions Web Login extension:

1. Click on **Devolutions Web Login** * extension at the top right corner of your browser.



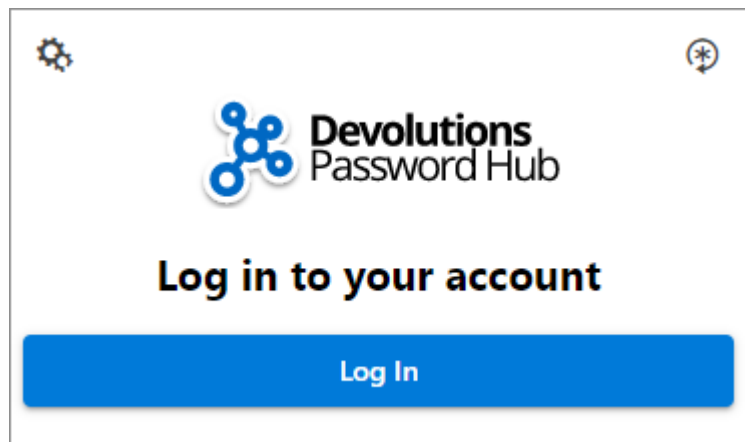
A Devolutions Password Hub access is required to continue.

2. Choose **Devolutions Password Hub** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



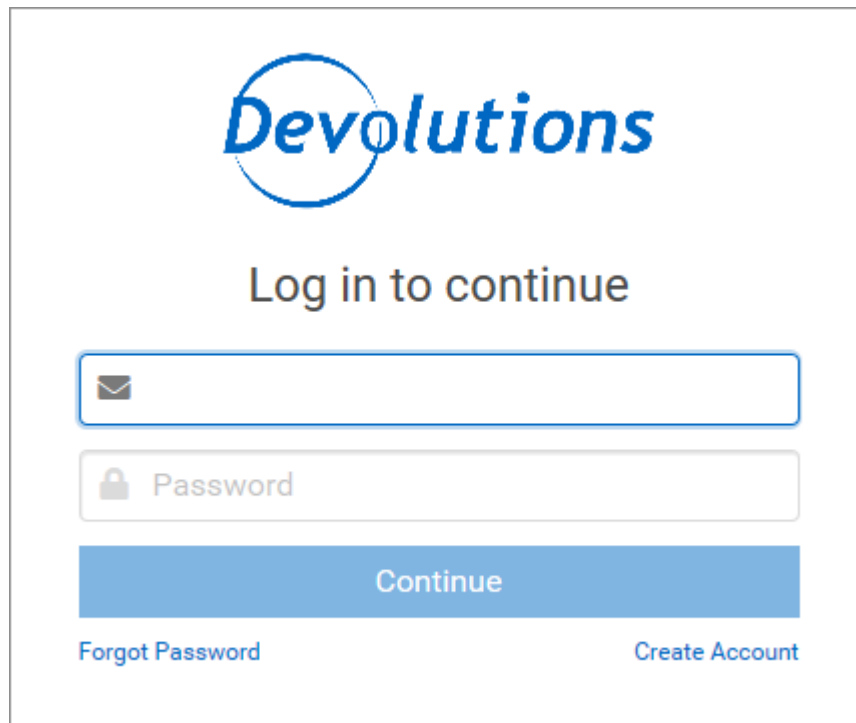
First Login

3. **Log in** to your account.




Log In

4. Enter the credentials from your Devolutions Account to continue.

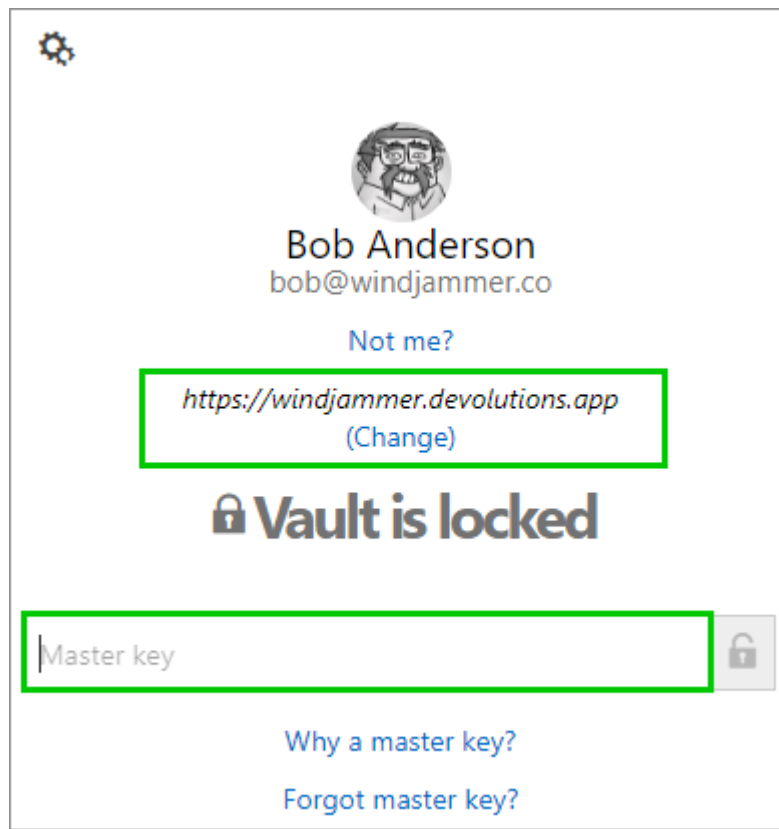
The image shows a login form for Devolutions. At the top is the "Devolutions" logo in blue. Below it is the text "Log in to continue". There are two input fields: the first has an envelope icon and is for email, and the second has a lock icon and is labeled "Password". Below these fields is a blue button with the text "Continue". At the bottom left is a link "Forgot Password" and at the bottom right is a link "Create Account".

Devolutions Account Login

5. Unlock the vault with your master key.



Devolutions Web Login will recognize automatically the Password Hub linked to your Devolutions account. Click **Change** to modify the URL.



The screenshot shows a web login interface for Devolutions. At the top left is a gear icon. In the center is a circular profile picture of a man with glasses and a beard. Below the picture is the name "Bob Anderson" and the email "bob@windjammer.co". A blue link "Not me?" is below the email. A green box highlights the URL "https://windjammer.devolutions.app" with a "(Change)" link below it. Below this, the text "Vault is locked" is displayed with a padlock icon. A green box highlights a text input field containing "Master key" with a padlock icon to its right. At the bottom are two blue links: "Why a master key?" and "Forgot master key?".

Bob Anderson
bob@windjammer.co

[Not me?](#)

<https://windjammer.devolutions.app>
[\(Change\)](#)

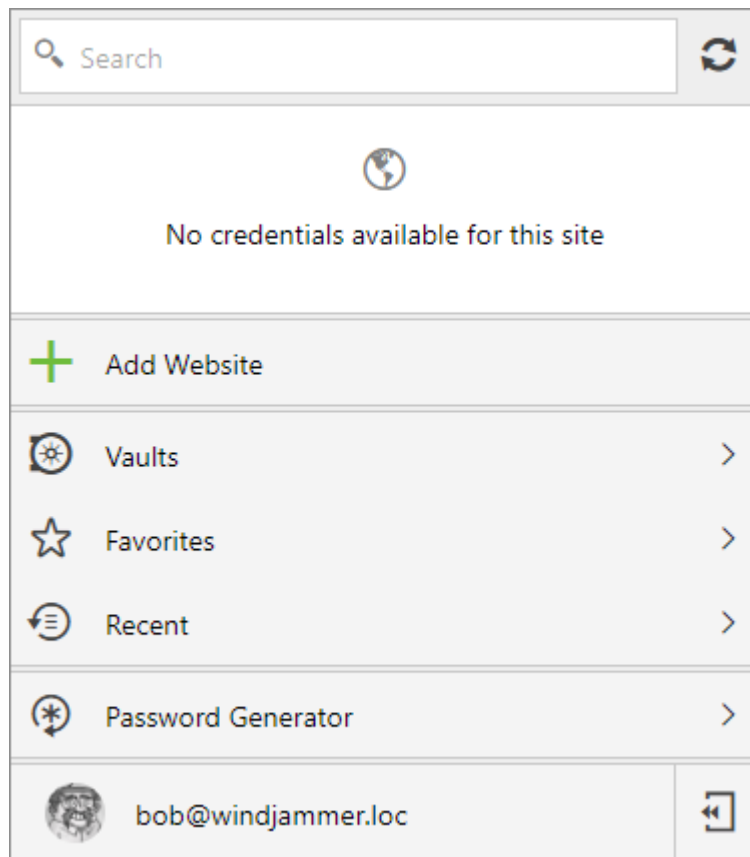
Vault is locked

Master key

[Why a master key?](#)
[Forgot master key?](#)

Password Hub Master key

Devolutions Web Login is now connected to your vaults.



Devolutions Web Login Connected to Devolutions Password Hub

7.3.1.1 Multiple Password Hub

DESCRIPTION

MANAGING MULTIPLE PASSWORD HUB WITH DEVOLUTIONS WEB LOGIN

Devolutions Web Login will automatically acknowledge all Password Hub linked to your Devolutions account.

- [View active Password Hub](#)
- [Switch Password Hub in Devolutions Web Login](#)

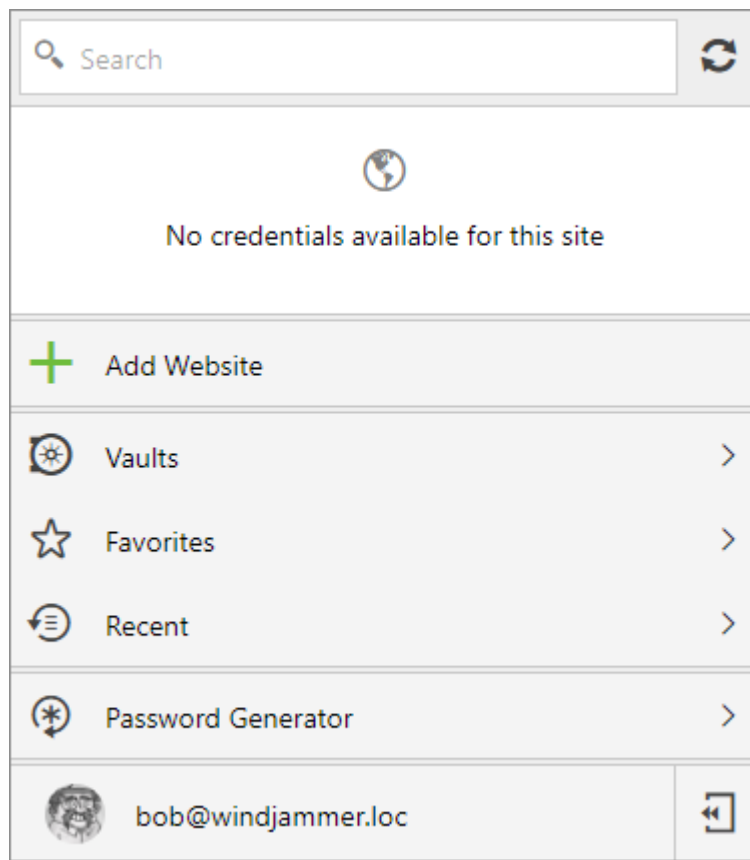


Devolutions Web Login will only recognize and apply credentials from the **active** Password Hub.

VIEW ACTIVE PASSWORD HUB

To view/validate the active Password Hub, click on the **Devolutions Web Login *** extension at the top right corner of your browser.

1. Click on your avatar at the bottom of the window.



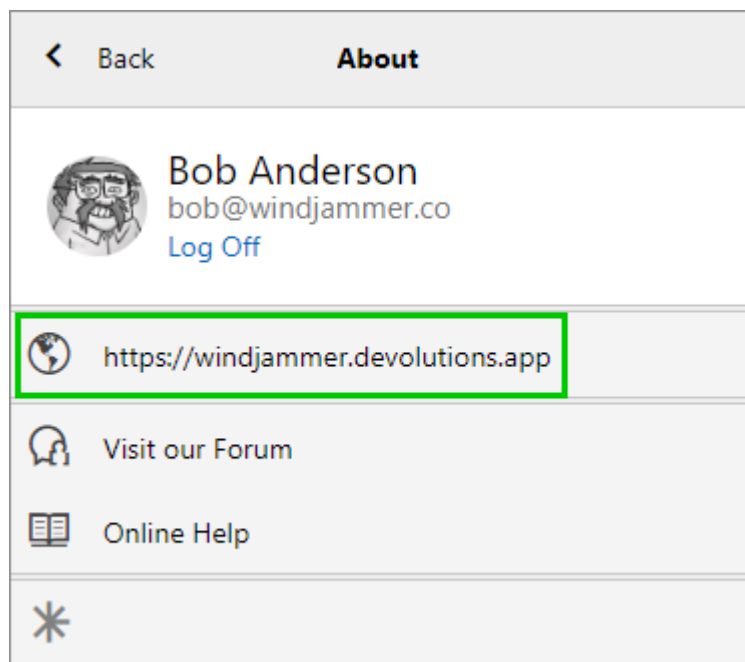
Devolutions Web Login

2. Click **About**.



Devolutions Web Login About

3. Validate the Password Hub URL.

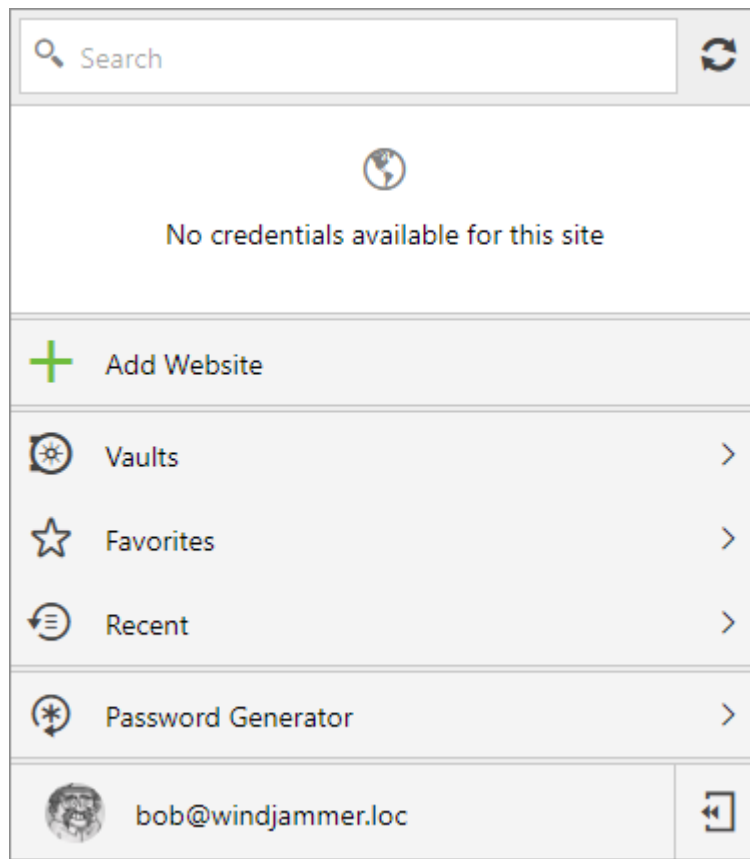


Password Hub URL

SWITCH PASSWORD HUB IN DEVOLUTIONS WEB LOGIN

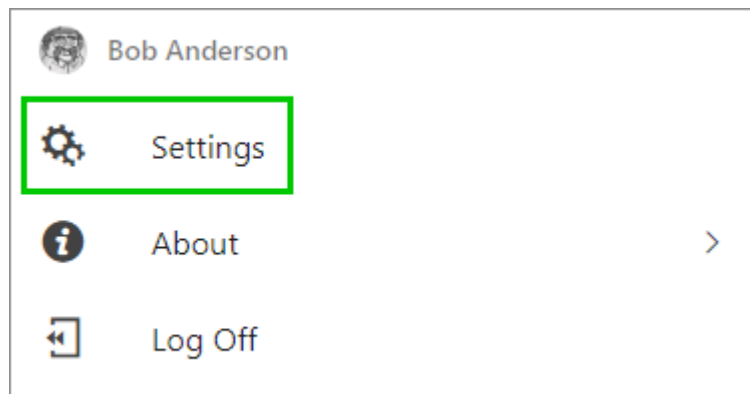
To switch Password Hub in Devolutions Web Login, click on the **Devolutions Web Login** * extension at the top right corner of your browser.

1. Click on your avatar at the bottom of the window.



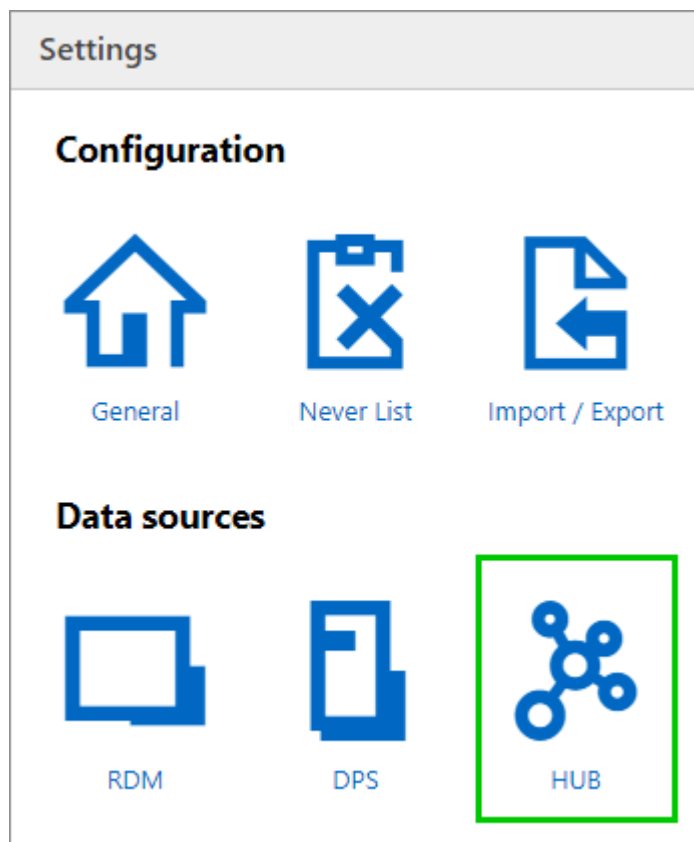
Devolutions Web Login

2. Click **Settings**.



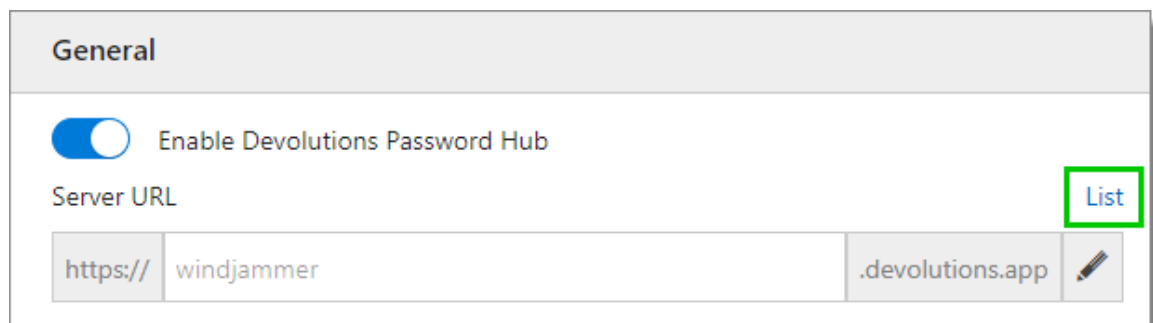
Devolutions Web Login Settings

3. Click **HUB**.



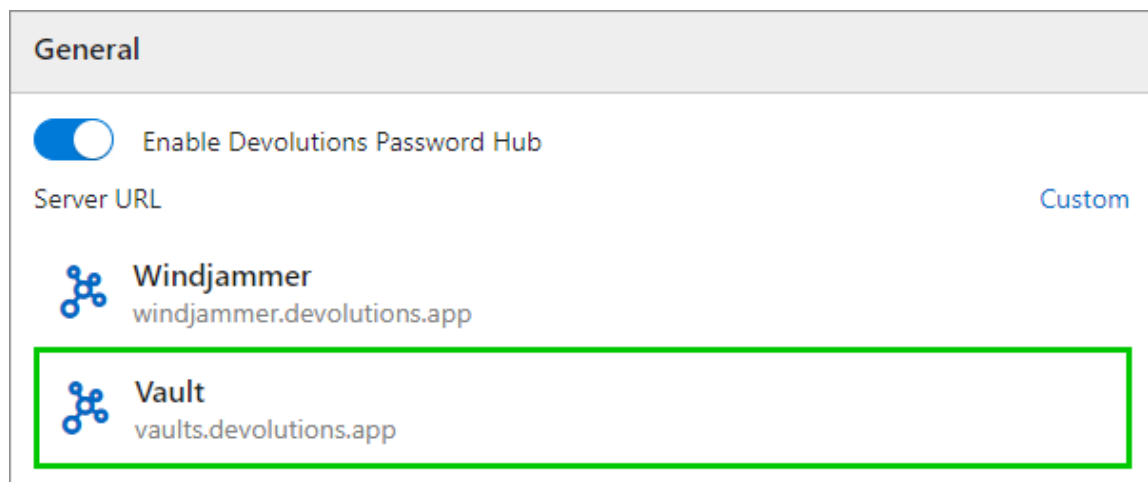
Devolutions Web Login Settings Menu

4. In the **General** section, click **List**.



Devolutions Web Login General Settings


5. All the available Password Hub linked to your Devolutions account will show in the list. Switch by clicking once on the desired Password Hub.




General

☒ Enable Devolutions Password Hub

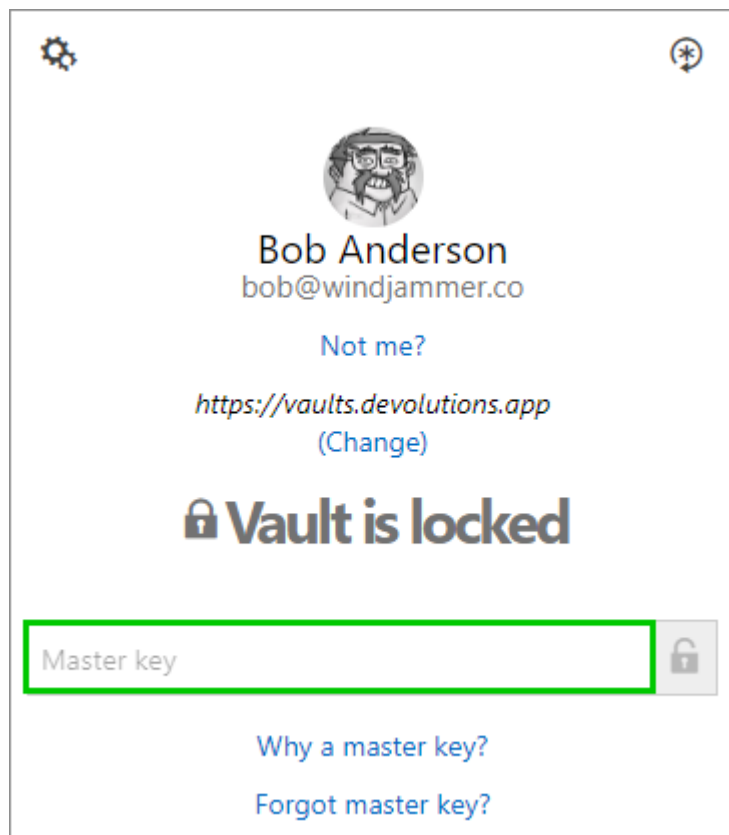
Server URL Custom



 **Windjammer**
windjammer.devolutions.app


 **Vault**
vaults.devolutions.app

Password Hub List

6. Click on the **Devolutions Web Login** * extension at the top right corner of your browser and enter the Master key associated with this Password Hub.





 


Bob Anderson
bob@windjammer.co

[Not me?](#)

<https://vaults.devolutions.app>
[\(Change\)](#)

 **Vault is locked**



[Why a master key?](#)

[Forgot master key?](#)

Password Hub Switch Master key

7.3.2 Password Server

DESCRIPTION

FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

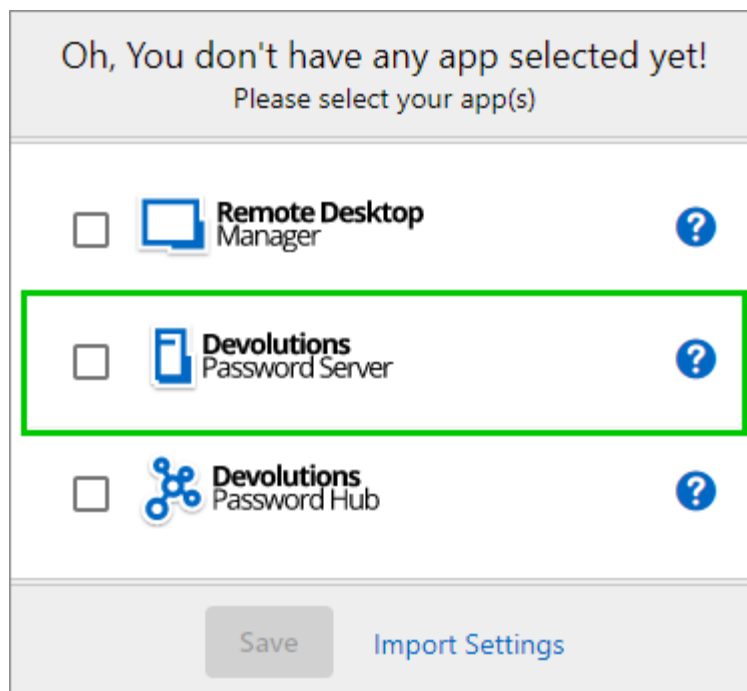
Follow these steps to connect Devolutions Password Server to Devolutions Web Login extension:

1. Click on **Devolutions Web Login** * extension at the top right corner of your browser.



A Devolutions Password Server access is required to continue.

2. Choose **Devolutions Password Server** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



First Login

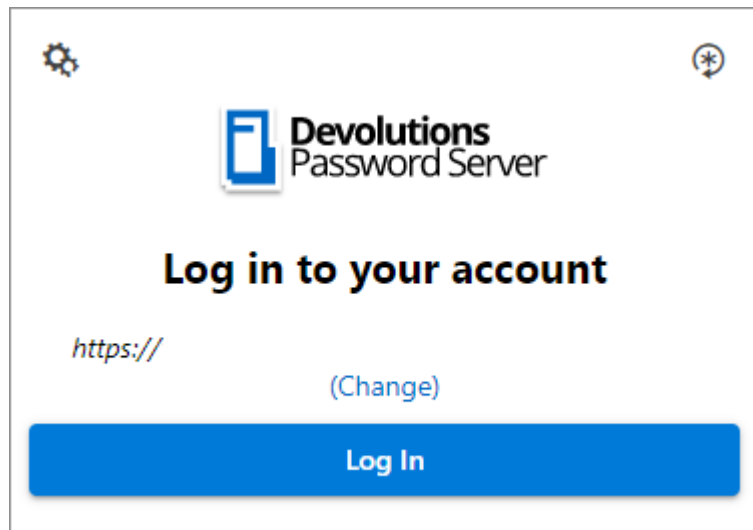
3. Enter the server address. Test the connection to validate it, then **Save**.



The screenshot shows a window titled "Devolutions Password Server". At the top left is a gear icon and at the top right is a lock icon. The main heading is "Please enter the server address". Below this is a text input field. At the bottom are two buttons: "Test Connection" and "Save".

Server Address

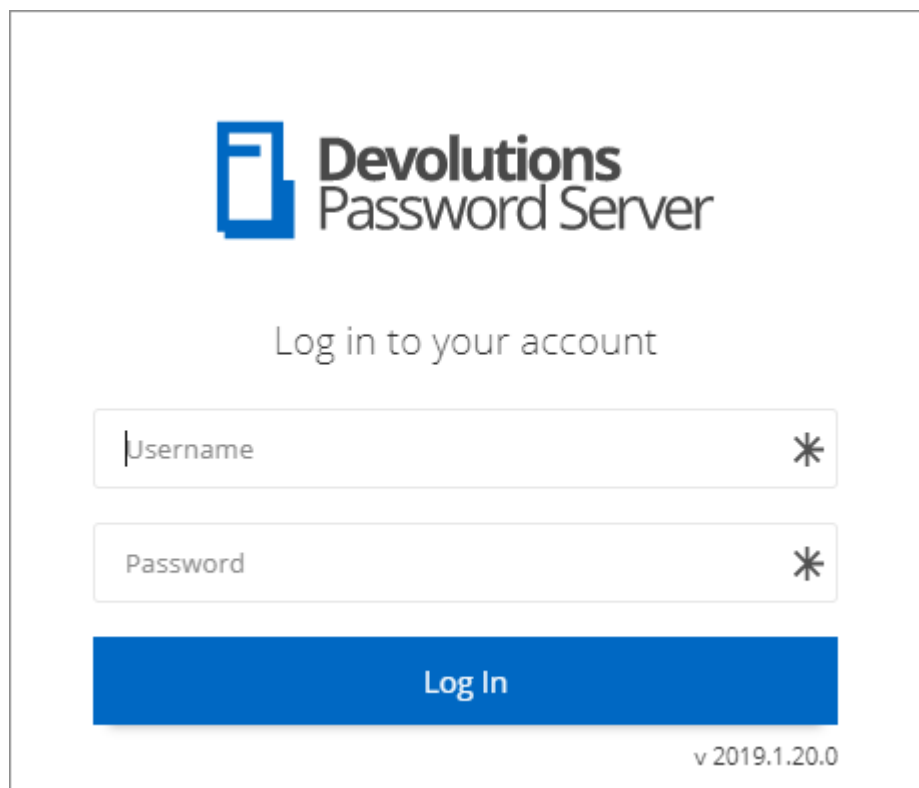
4. Press the **Log In** after you saved the address.



The screenshot shows the same window as before, but the heading is now "Log in to your account". Below the heading is the text "https://" followed by a "(Change)" link. At the bottom is a large blue button labeled "Log In".

Devolutions Web Login Login

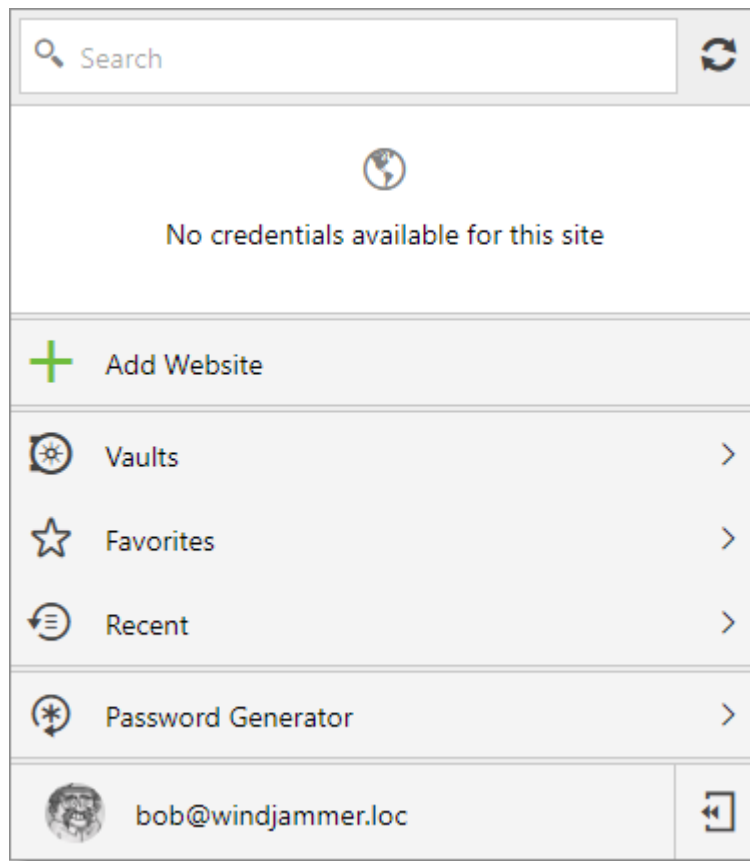
5. Enter your Devolutions Password Server credentials and log in.



The image shows a login window for Devolutions Password Server. At the top is the logo, which consists of a blue square icon with a white 'D' shape inside, followed by the text 'Devolutions Password Server'. Below the logo is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small asterisk icon on the right side. Below the input fields is a large blue button with the text 'Log In'. In the bottom right corner of the window, the version number 'v 2019.1.20.0' is displayed.

Devolutions Password Server Login

Devolutions Web Login is now connected to your vaults.



Devolutions Web Login Connected

7.3.3 Remote Desktop Manager

DESCRIPTION

FIRST LOGIN WITH DEVOLUTIONS WEB LOGIN

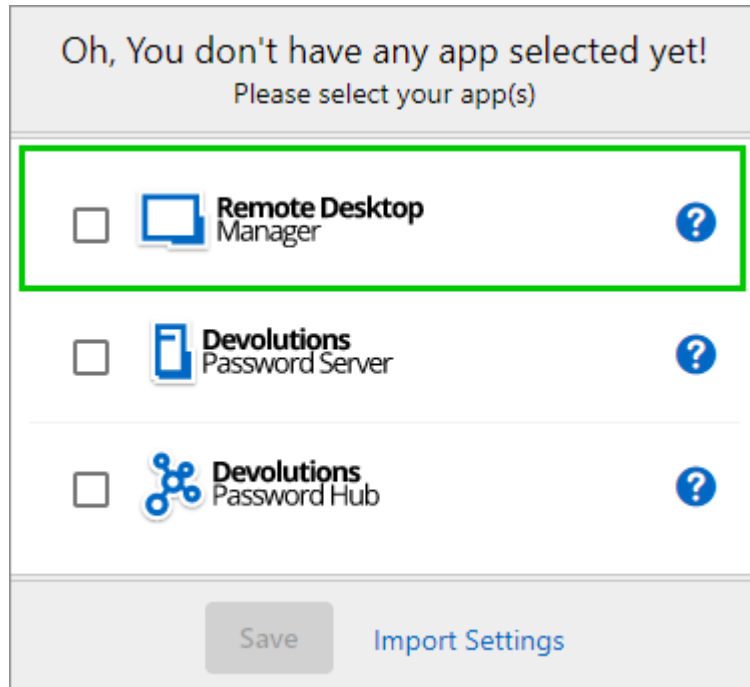
Follow these steps to connect your Remote Desktop Manager to Devolutions Web Login extension:

1. Click on Devolutions Web Login * extension at the top right corner of your browser.



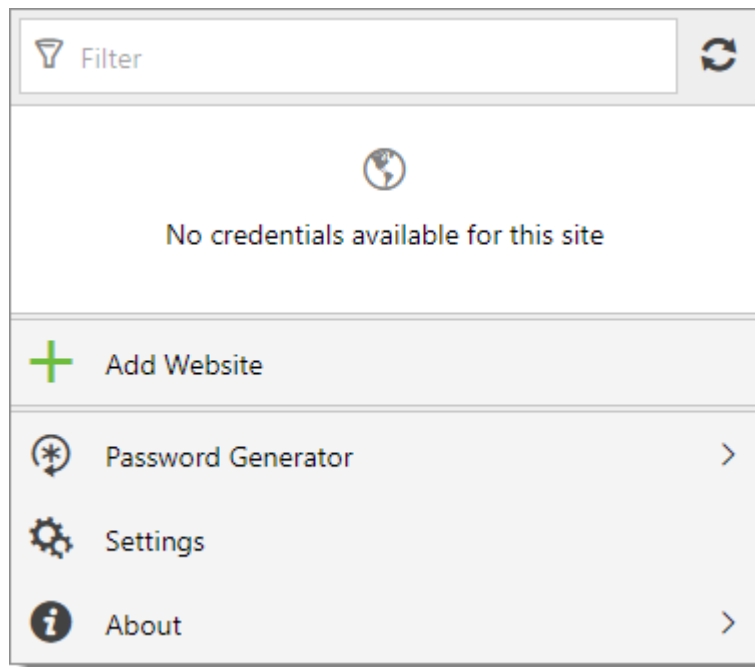
Remote Desktop Manager must be installed and running to continue.

2. Choose **Remote Desktop Manager** in the list and **Save**. You could at this point import settings; the option will also be available in the [Settings](#) menu after the log in.



First Login

You will be automatically connected to your vaults.



Devolutions Web Login Connected

7.4 Exploring Devolutions Web Login

7.4.1 Menu

DESCRIPTION

The user interface **Devolutions Web Login** is slightly different in appearance when connected to Remote Desktop Manager, Devolutions Password Server or Devolutions Password Hub.

See below a list of the menu and information available from the Devolutions Web Login extension:

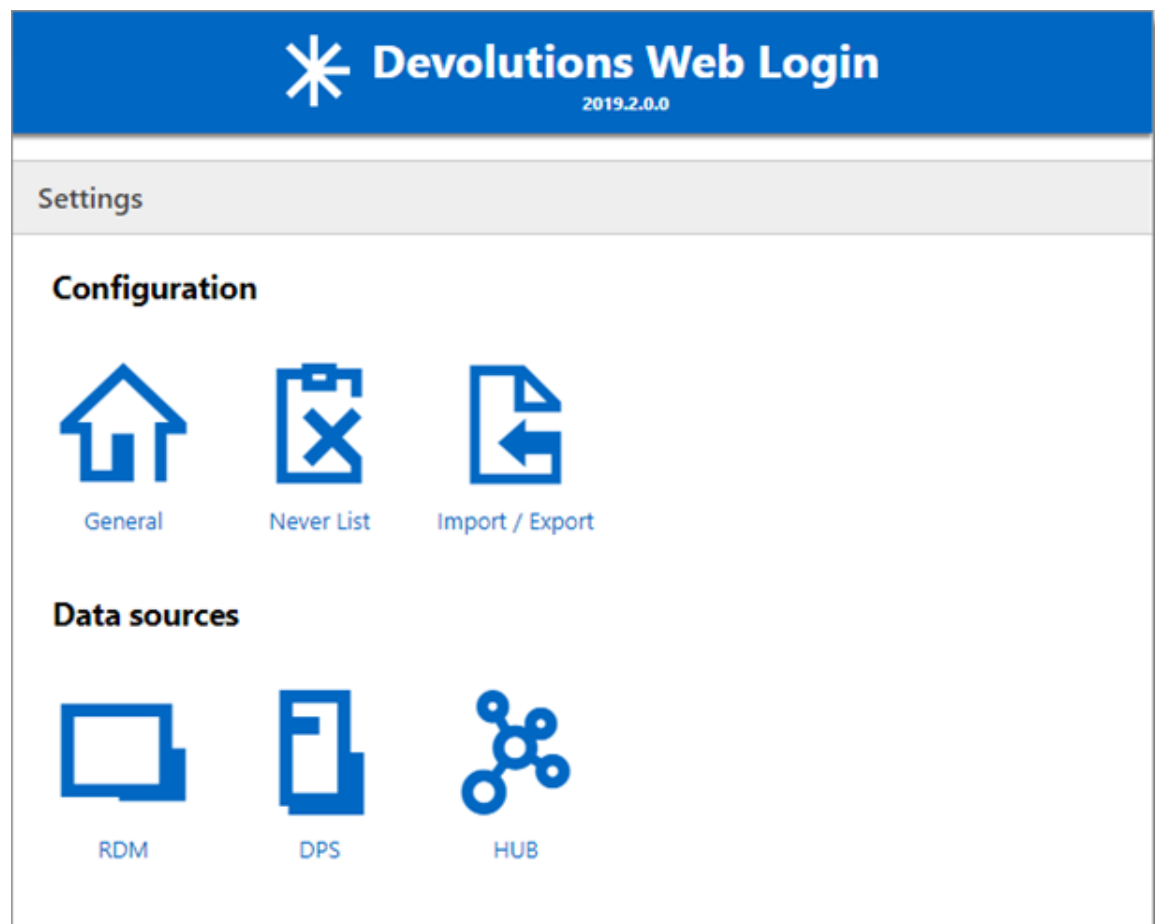
- Refine the credential list available with the **search**.
- **Add a website** from Devolutions Web Login in a specific folder located in a vault or your personal vault.
- **Visualize the credential** stored in the vaults if you are connected with Devolutions Password Server or Devolutions Password Hub.
- Browse **recently used entry** or **favorites**.

- Use the **password generator** to create custom and more secure credentials.
- Set Devolutions Web Login [settings](#).

7.4.1.1 Settings

DESCRIPTION

Devolutions Web Login settings are separated in two categories, [Configuration](#) and [Data sources](#).



Devolutions Web Login Settings

CONFIGURATION

The **General** settings are about the user interface and interaction.

- Show Devolutions Web Login extension icon in the credentials fields.
- Show the prompt when saving credentials on new login.
- Color the fields that are filled with Devolutions Web Login
- Disable the analytics in the advanced setting.

The **Never list** displays the list of websites, added locally, to which the user will never be prompted to save credentials.

- Type can range from: Never add site, Never autofill, Never do anything too Never show icons in field.
- Matching options are: Base domains, Host, Starts with, RegEx and Exact.

To remove a website from the never list click the **trash can** icon next to it. To edit an entry, delete it and create another.

The **Import / Export** setting allows to save and transfer your currently set preferred settings.

- Import setting from other browsers or users.
- Choose to export Devolutions Web Login settings, password generator template and the never list.

DATA SOURCES

The data sources settings are used to customize Devolutions Web Login interactions with [Remote Desktop Manager](#), [Devolutions Password Server](#) and [Devolutions Password Hub](#).

REMOTE DESKTOP MANAGER

GENERAL OPTIONS	DESCRIPTION
Enable Remote Desktop	Retrieve entries from Remote Desktop Manager

GENERAL OPTIONS	DESCRIPTION
Manager app	when the application is open.
Use default port (19443)	Communicate with the default port 19443 between the application.
Add entry in personal vault by default	Save new entries in the personal vault.
Destination folder	Choose the folder where the credentials are stored in the vault.
ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled.
ADVANCED OPTIONS	DESCRIPTION
Application key	<p>Secure the port with an application key by using the same code in Remote Desktop Manager and Devolutions Web Login.</p> <p>Navigate to File – Options – Browser Extensions in Remote Desktop Manager to set the application key.</p>

ADVANCED OPTIONS	DESCRIPTION
Enable native messaging	Exchange messages with a native application installed on the user's computer.
Use legacy API	Use the old browser extension API for compatibility with older versions of Remote Desktop Manager.

DEVOLUTIONS PASSWORD SERVER

GENERAL OPTIONS	DESCRIPTION
Enable Devolutions Password Server	Retrieve entries from Devolutions Password Server.
Destination folder	Choose the folder where the credentials are stored in the vault.
Server URL	Enter the URL of the Devolutions Password Server instance to connect to.

ACTION OPTIONS	DESCRIPTION
Automatically retrieve credentials on page load	<p>Devolutions Web Login automatically search for credentials in the data source when connecting to a website.</p> <p>If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.</p>
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled.

DEVOLUTIONS PASSWORD HUB

GENERAL OPTIONS	DESCRIPTION
Enable Devolutions Password Hub	Retrieve entries from Devolutions Password Hub.
Server URL	Enter the URL of the Devolutions Password Hub instance to connect to.
ACTION OPTIONS	DESCRIPTION
Automatically fill in credentials on load	Fill automatically the credentials when loading a web page.
Automatically submit the form after filling	Submit the credentials automatically when the fields are filled
ADVANCED OPTIONS	DESCRIPTION
Devolutions Account login	Set your Devolutions Account login URL.
Show favicon	Display the Devolutions Web Login favicon.

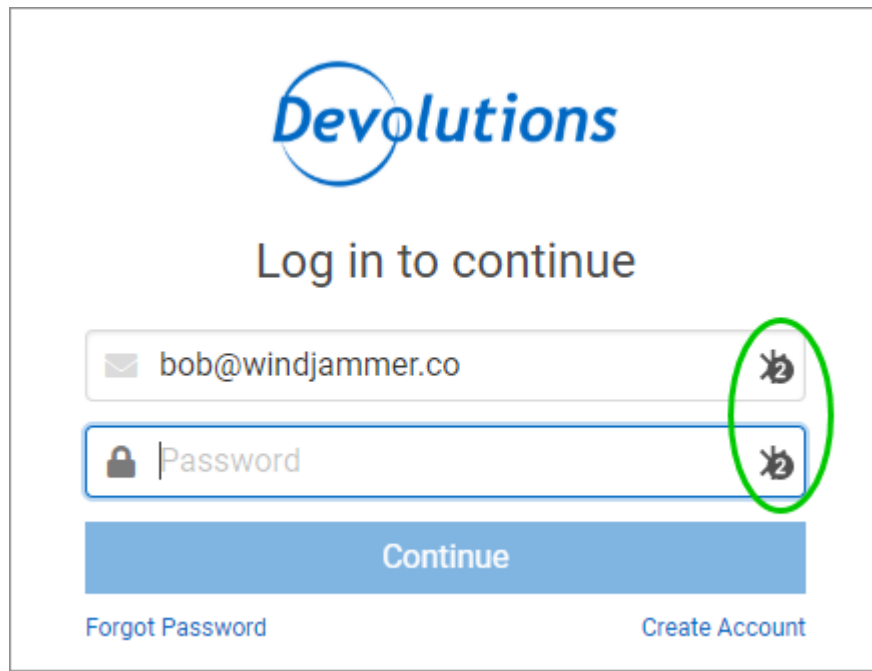
7.4.2 Retrieve Credentials

DESCRIPTION

Once configured in your Devolutions product, credentials are automatically detected by **Devolutions Web Login** when connected to their respective applications.

LOG IN TO A WEBSITE

Select an entry from the list in Devolutions Web Login or click on the icon in the credential field to fill in the login information and connect to the website.

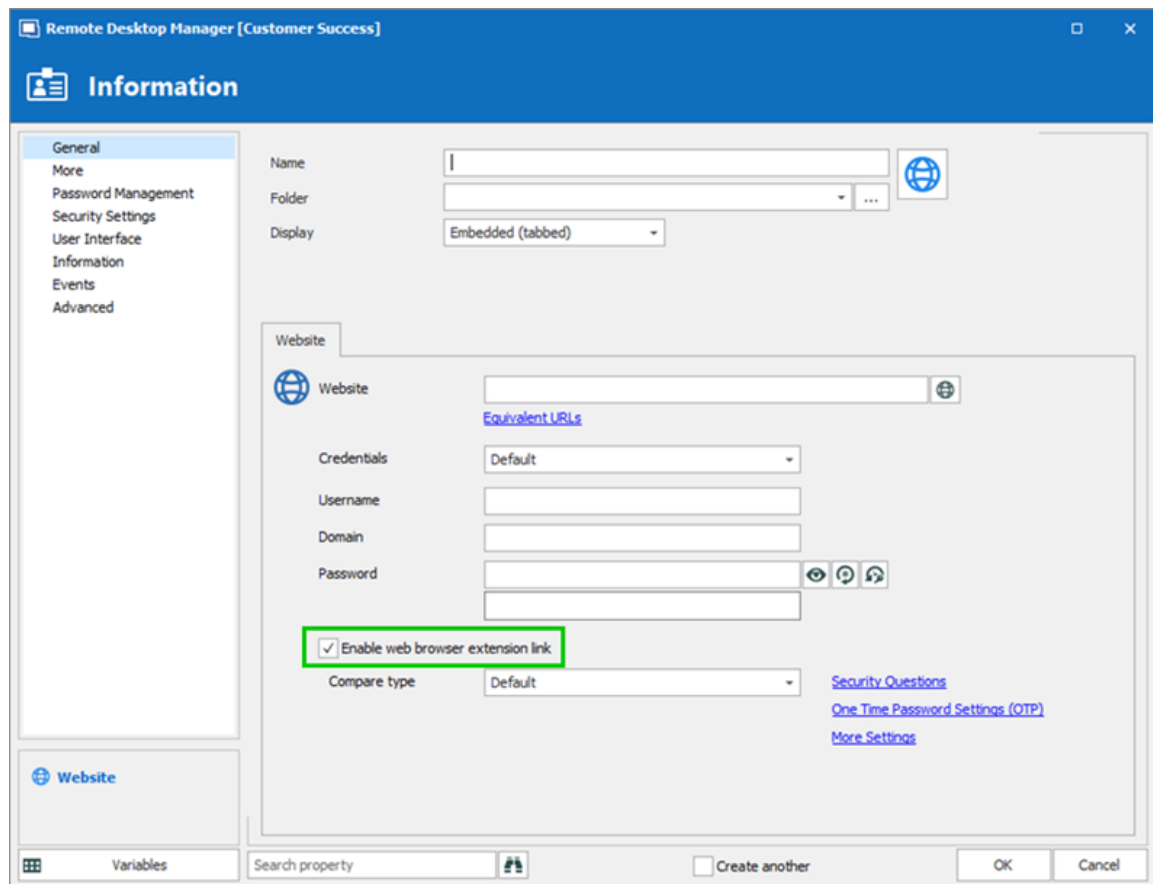
The image shows the Devolutions Web Login interface. At the top is the Devolutions logo. Below it is the text "Log in to continue". There are two input fields: the first is for an email address, containing "bob@windjammer.co", and the second is for a password, containing the text "Password". Both input fields have a small icon on the right side, which is circled in green. Below the input fields is a blue "Continue" button. At the bottom, there are two links: "Forgot Password" on the left and "Create Account" on the right.

Automatic Log In

7.4.2.1 Remote Desktop Manager

DESCRIPTION

Checkmark ***Enable web browser extension link*** in Remote Desktop Manager entries to allow Devolutions Web Login extension to retrieve the credentials when connecting to its respective website.



Enable web browser extension link

7.4.3 Secure Devolutions Web Login

DESCRIPTION

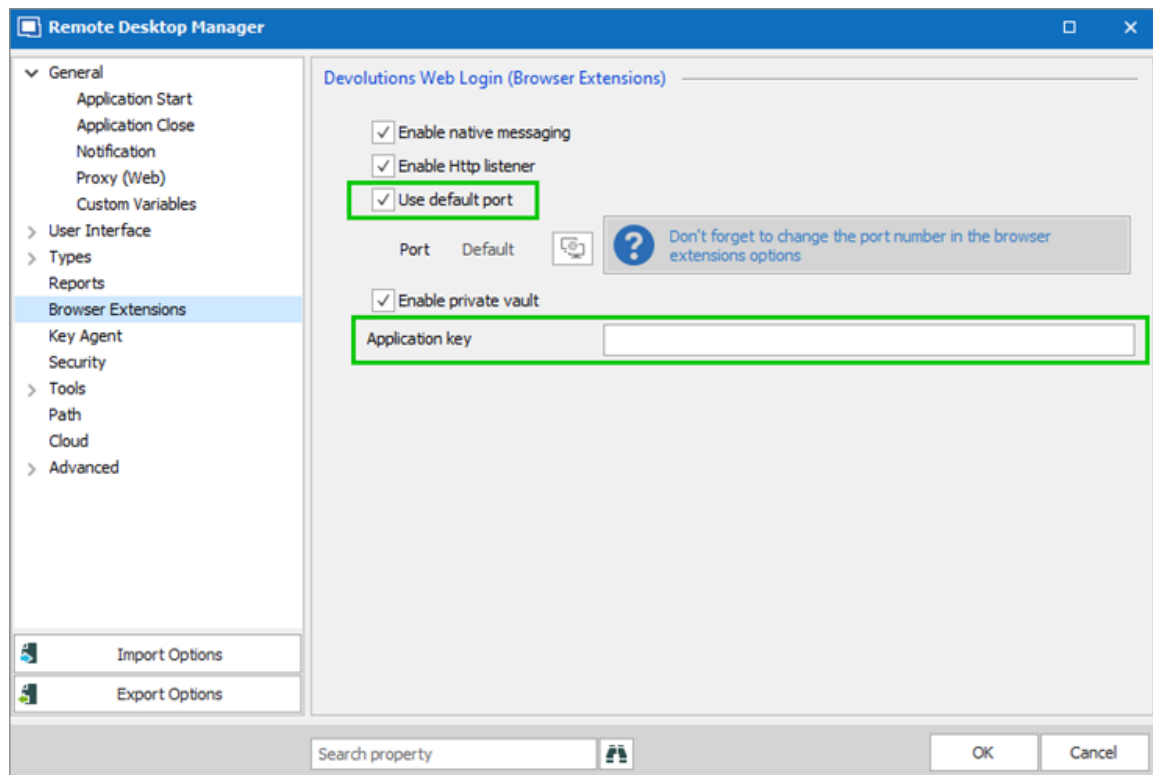
As mentioned in the Devolutions Web Login [Overview](#) topic, installing the extension in a Terminal Services environment can introduce security risks. In such environments, each user must have a distinct port assigned, as well as an application key to prevent any other Devolutions Web Login from listening in.



The application key is displayed in clear text, it must be kept secret by the user.

To enable the security layer in Remote Desktop Manager, follow these steps:

1. Navigate to **File – Options – Browser Extensions**.
2. Uncheck **Use default port**.
3. Enter a custom port.
4. Type an **Application key** then click **OK**



Remote Desktop Manager Browser Extensions Options

5. In your browser, click the Devolutions Web Login icon * and go to Remote Desktop Manager Settings.
6. Disable **Use default port**.
7. Enter the custom port created earlier in Remote Desktop Manager.
8. Enter the same **Application key** as Remote Desktop Manager .

Devolutions Web Login
2019.2.2.0

Settings > RDM

General

☒ Enable Remote Desktop Manager app

☐ Use default port (19443)

Port
19443

☒ Add entry in private vault by default

Destination folder
Devolutions Products

Actions

☒ Automatically retrieve credentials on page load

☒ Automatically fill in credentials on load

☐ Automatically submit the form after filling

Advanced

Application key

☐ Enable native messaging

☐ Use legacy API

Devolutions Web Login Settings for Remote Desktop Manager

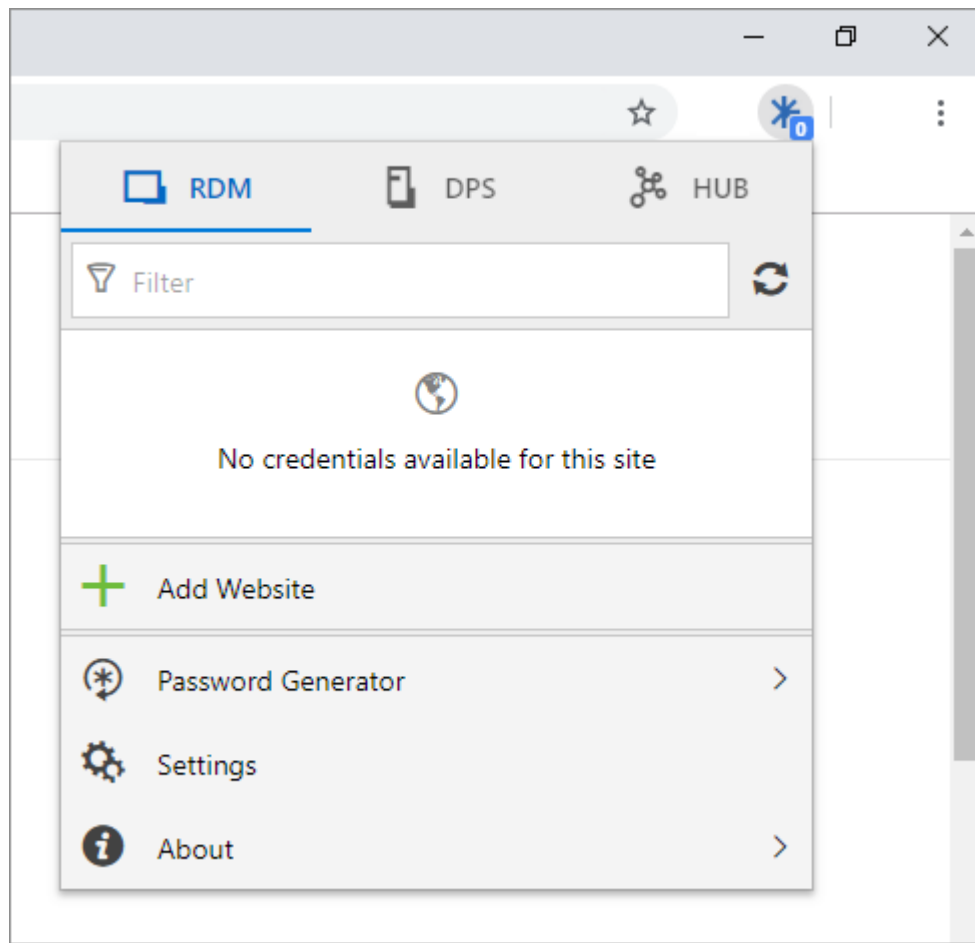
7.4.4 Keyboard Shortcuts

DESCRIPTION

Here is the list of keyboard shortcuts available for Devolutions Web Login:

CTRL+SHIFT+Z

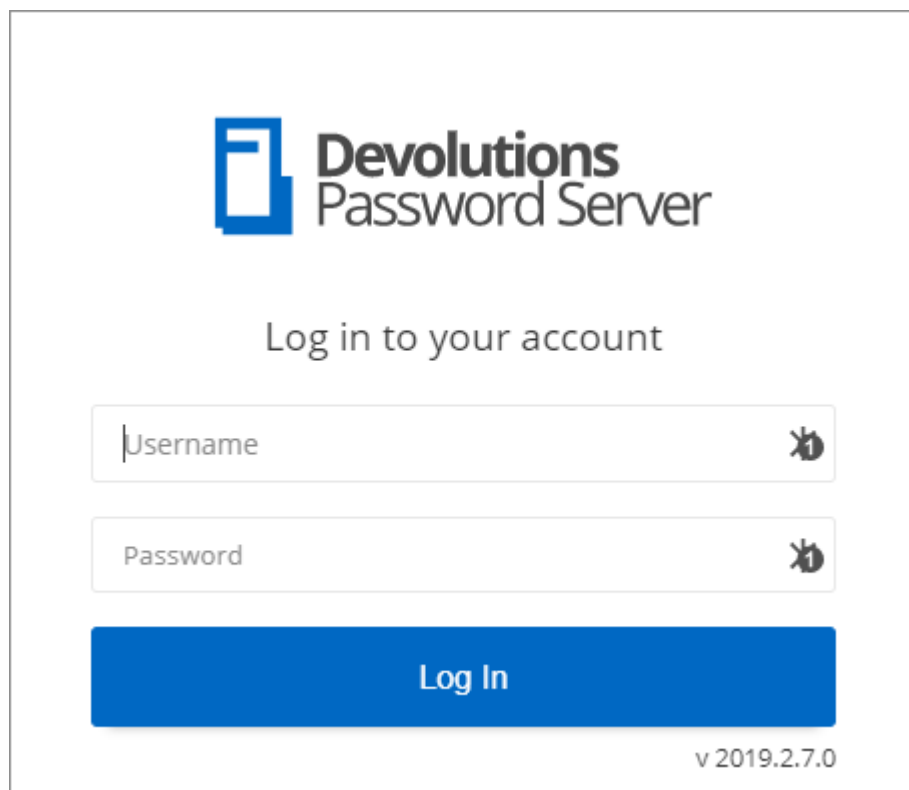
Use this key shortcut to open Devolutions Web Login window in your active browser.



Devolutions Web Login in Chrome

CTRL+SHIFT+Y

Use it to auto-fill your credential when only one is available for an entry.

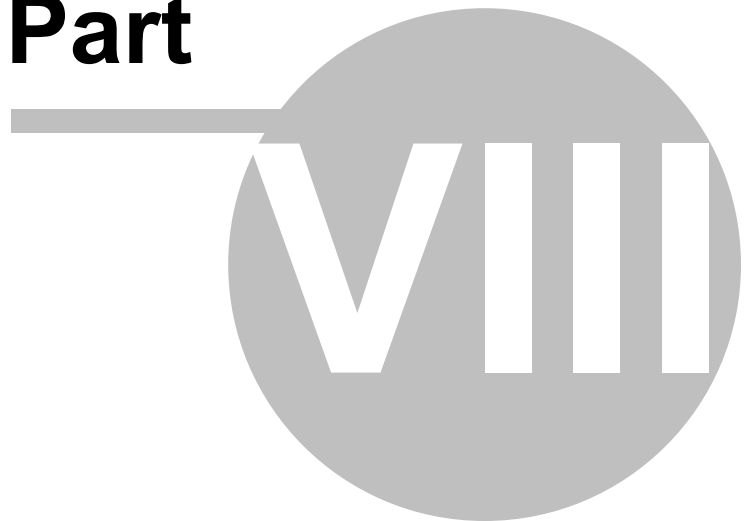


The image shows a login window for Devolutions Password Server. At the top is the logo, which consists of a blue square icon with a white stylized 'D' and the text 'Devolutions Password Server' in a sans-serif font. Below the logo is the instruction 'Log in to your account'. There are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields have a small icon on the right side, which appears to be a key or a similar symbol. Below the input fields is a large blue button with the text 'Log In' in white. In the bottom right corner of the window, the version number 'v 2019.2.7.0' is displayed.

One Credential Login with Devolutions Web Login

Devolutions Launcher

Part





8 Devolutions Launcher

8.1 Overview



Devolutions Launcher is a companion tool for Devolutions Password Server and Devolutions Password Hub. It can launch multiple remote sessions simultaneously, while giving system administrators full control. It is available on Windows, macOS, Linux, Android and iOS.

 Devolutions Password Server Secure, Manage and Monitor Access to Privileged Accounts	 Devolutions Password Hub Vault and Manage Business-User Passwords
Devolutions Password Server lets you control access to privileged accounts and manage remote sessions through a secure solution that can be deployed on premises.	Devolutions Password Hub is a secure and cloud-based password manager for teams

8.2 Installation

8.2.1 Prerequisites

MINIMUM GENERAL REQUIREMENTS

Devolutions Password Server 2019.1.X.X or later.

Most recent browsers are supported and so is Internet Explorer 11 or above.

MINIMUM PLATFORM REQUIREMENTS

WINDOWS

- Windows 8 or later
- Microsoft .NET Framework 4.7.2
- 1 GHz or faster processor
- 2 GB of RAM
- 100 MB hard drive space

MACOS

- macOS X 10.12 or later
- 2 GB of RAM
- 150 MB hard drive space

LINUX

- Ubuntu 16.04
- 2 GB of RAM

- 250 MB hard drive space

ANDROID

- Android 6.0 or later
- API 23
- Download: 42 MB
- Device Family: Phone and Tablet

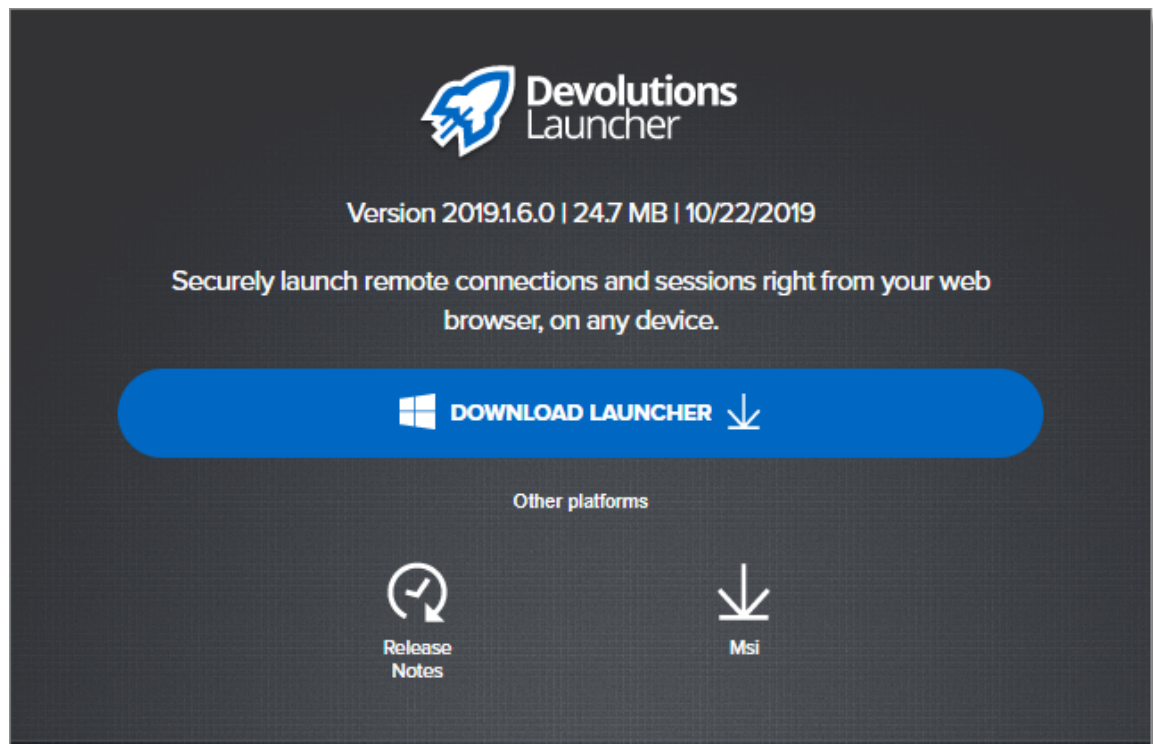
IOS

- iOS 10.3 or later
- Download size: 80 MB
- Device Family: iPhone, iPod touch and iPad

8.2.2 Windows

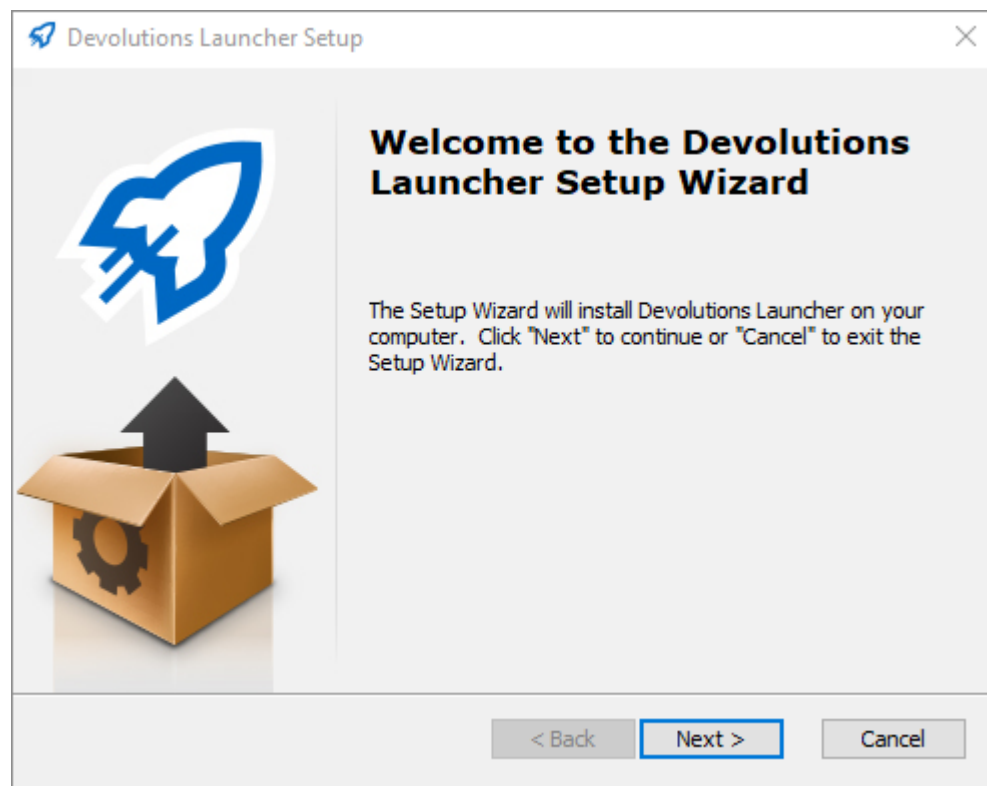
Follow these steps to install Devolutions Launcher:

1. Download [Devolutions Launcher](#) or search the companion tools in the products section of [Devolutions](#).



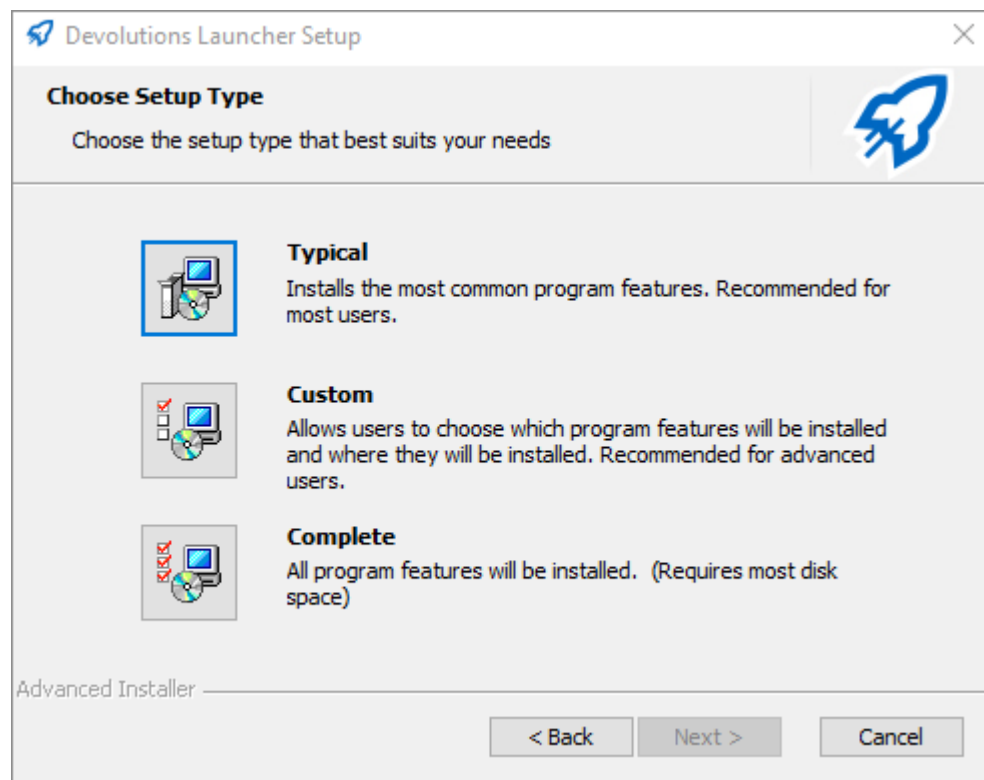
Devolutions Launcher Download Page

2. Open the downloaded file.
3. Click **Next** on the Welcome page.



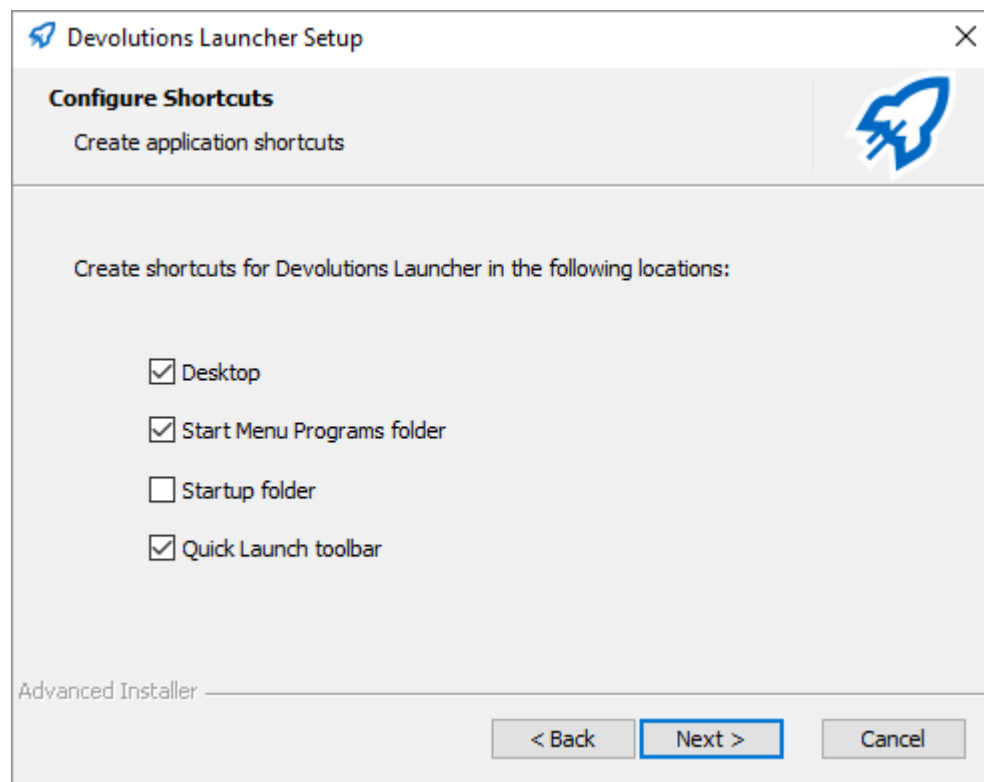
Devolutions Launcher Setup Wizard - Welcome

4. Choose the setup type.



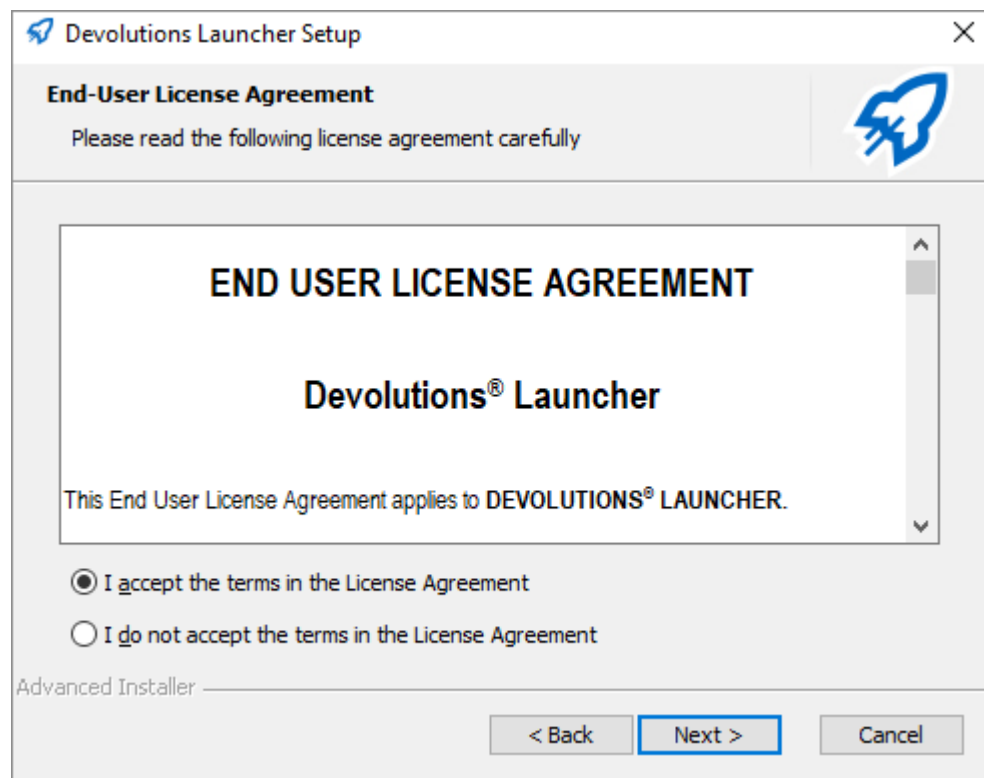
Devolutions Launcher Setup Wizard - Setup Type

5. Configure the shortcuts for Devolutions Launcher.



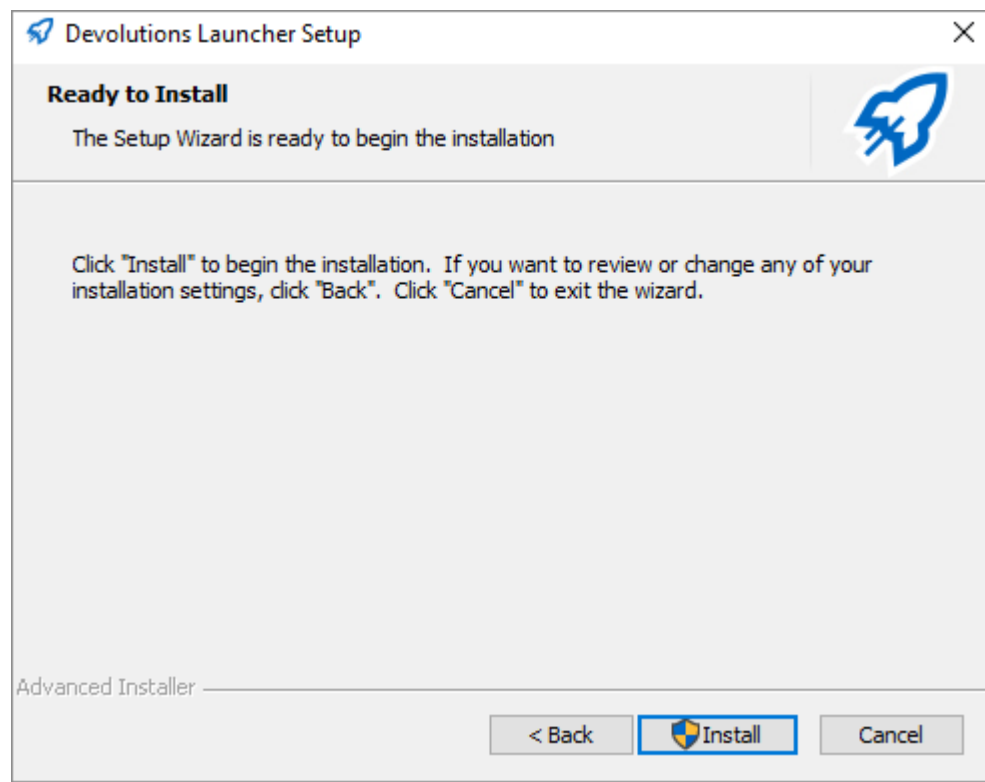
Devolutions Launcher Setup Wizard - Configure Shortcuts

6. Accept the terms of the license agreement and click **Next**.



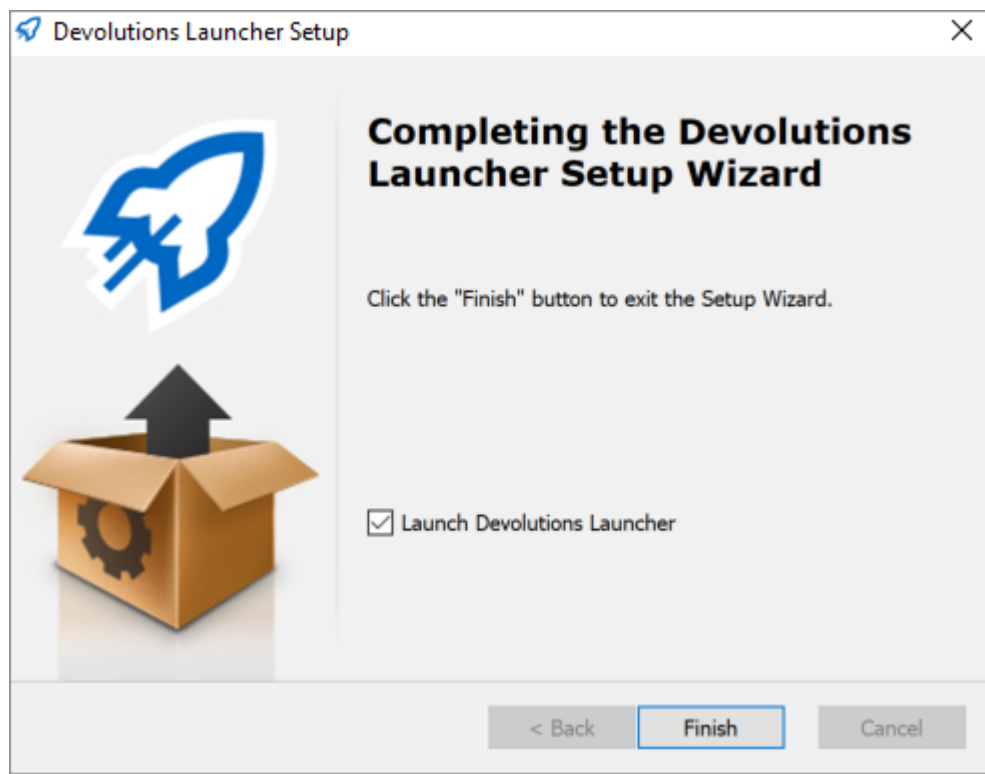
Devolutions Launcher - End User License Agreement

7. Click **Install**.



Devolutions Launcher - Ready to Install

8. Click **Finish** to complete the installation.



Devolutions Launcher - Complete

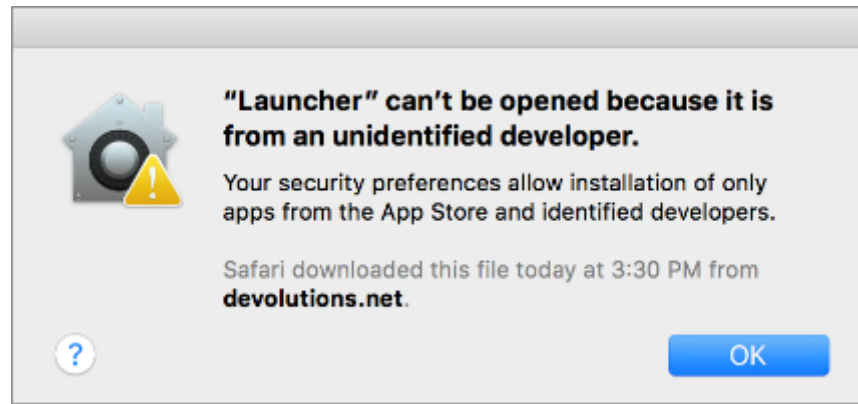
8.2.3 macOS

Follow these steps to install Devolutions Launcher:

1. Download [Devolutions Launcher](#) or search the companion tools in the products section of [Devolutions](#).
2. Open the downloaded file.
3. Drag the Devolutions Launcher icon into the application folder.

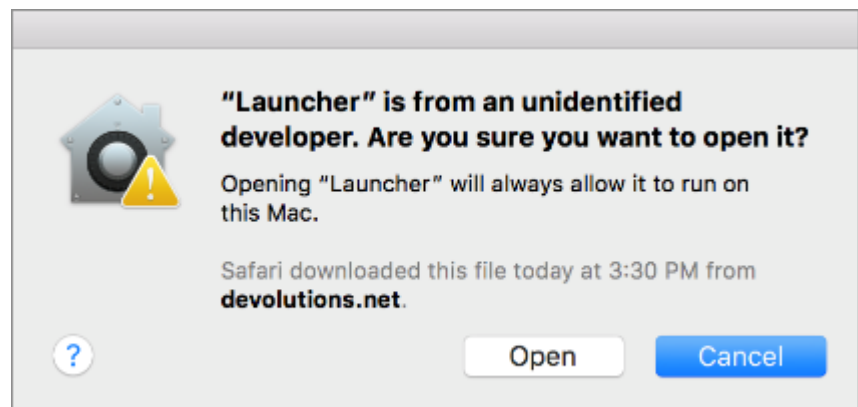


Follow these steps if at launch you get the warning that Devolutions Launcher can not be opened because it is from an unidentified developer:



Devolutions Launcher Unidentified Developer

1. Press **OK** to close the warning.
2. On the Devolutions Launcher icon in your application, press **control** and **click** to open the shortcut menu.
3. Click **Open**.
4. Click **Open** to the prompt to confirm.



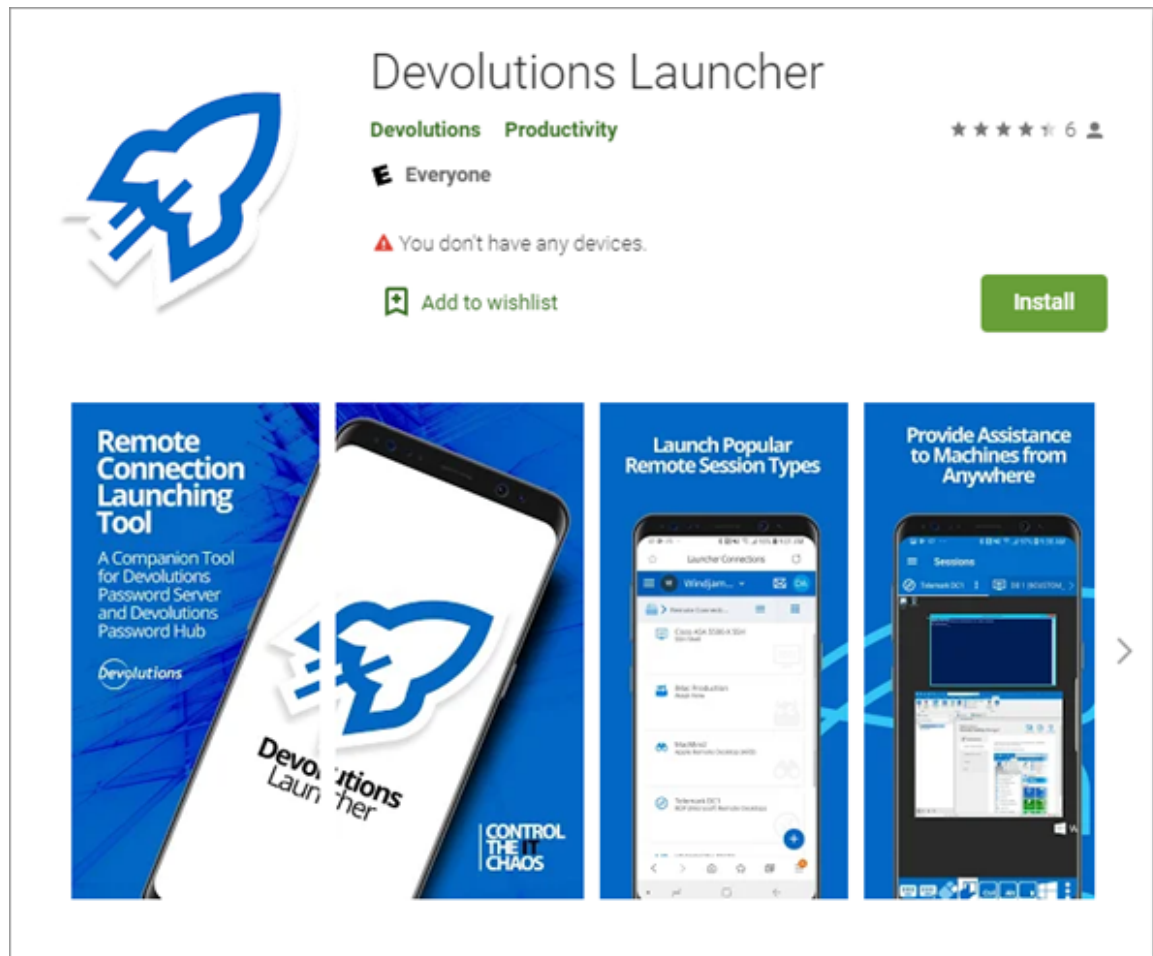
Devolutions Launcher Open Confirmation

You can also change your security preferences.

8.2.4 Android

Follow these steps to install Devolutions Launcher:

1. Download the [Devolutions Launcher](#) application or search for **Devolutions Launcher** in the Google Play Store.
2. Click **Install**.



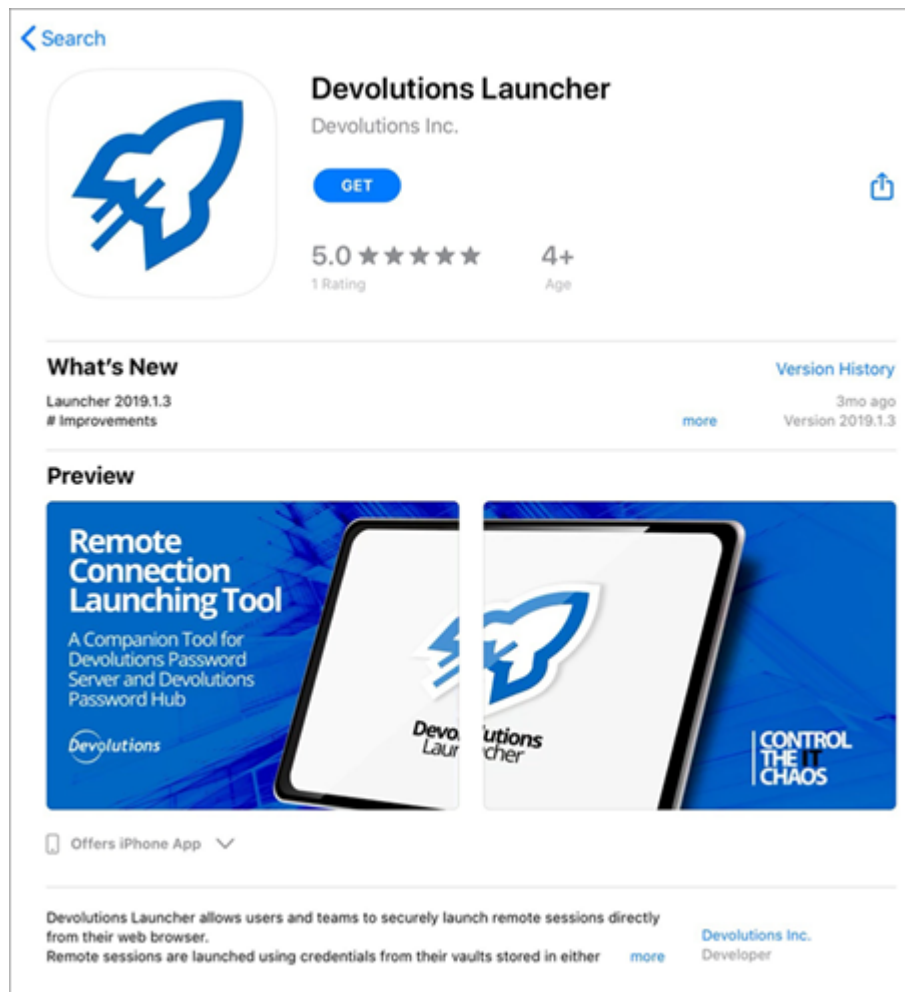
Devolutions Launcher in Google Play Store

3. Click **Open** when the download is complete.

8.2.5 iOS

Follow these steps to install Devolutions Launcher:

1. Search for **Devolutions Launcher** in the App Store.
2. Click **Get**, then **Install**.
3. Open the app.



Devolutions Launcher in the App Store

8.3 Configuration and Settings

8.3.1 Devolutions Password Server

Devolutions Launcher and Devolutions Password Server must be configured together. Launch connections can be set for all users in **Password Server Settings** or individually in **Account Settings**.

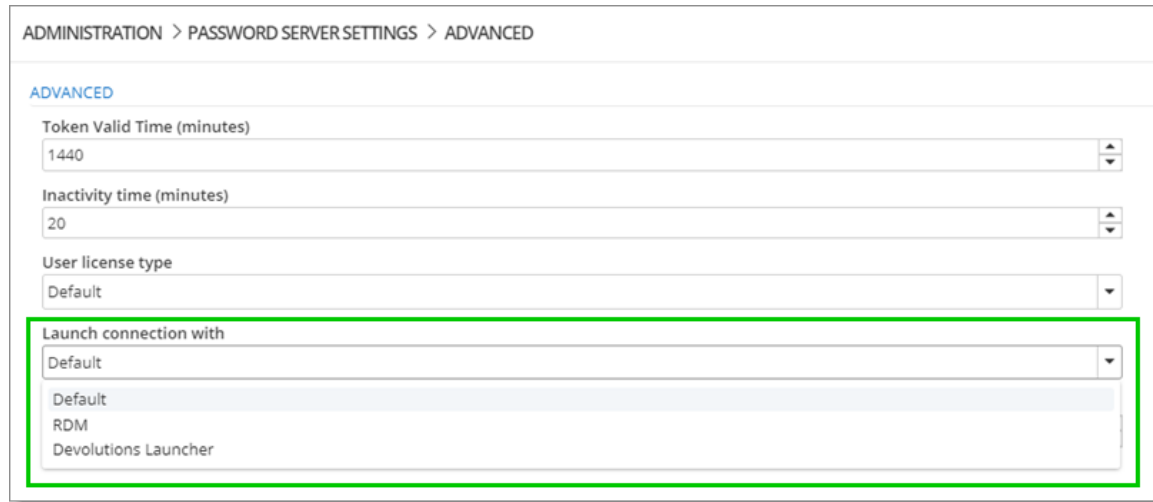


You need to at least log in to Devolutions Launcher **once** for the companion tool to launch your sessions from Devolutions Password Server.

SERVER SETTINGS

This method sets how all users open remote connections.

Choose Devolutions Launcher to open remote connections in **Administration – Password Server Settings – Advanced**.



ADMINISTRATION > PASSWORD SERVER SETTINGS > ADVANCED

ADVANCED

Token Valid Time (minutes)
1440

Inactivity time (minutes)
20

User license type
Default

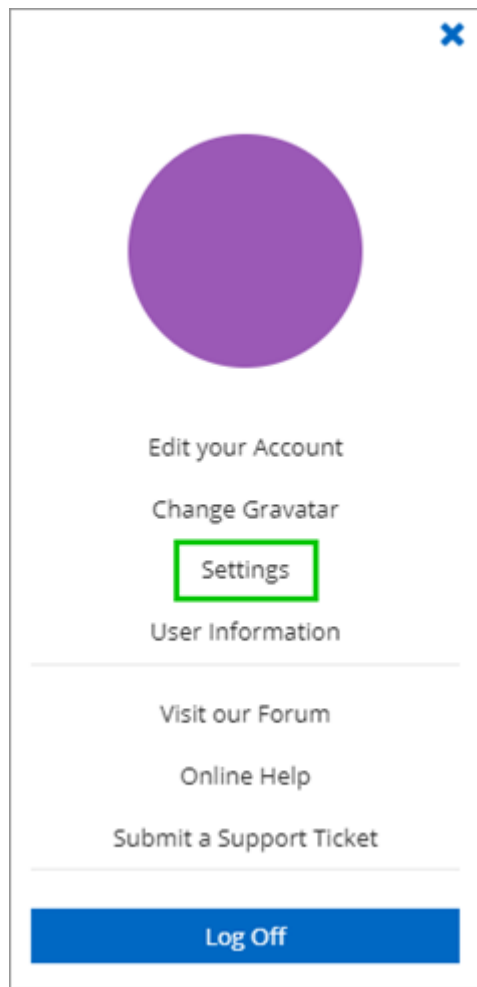
Launch connection with
Default
RDM
Devolutions Launcher

Administration – Password Server Settings – Advanced

ACCOUNT SETTINGS

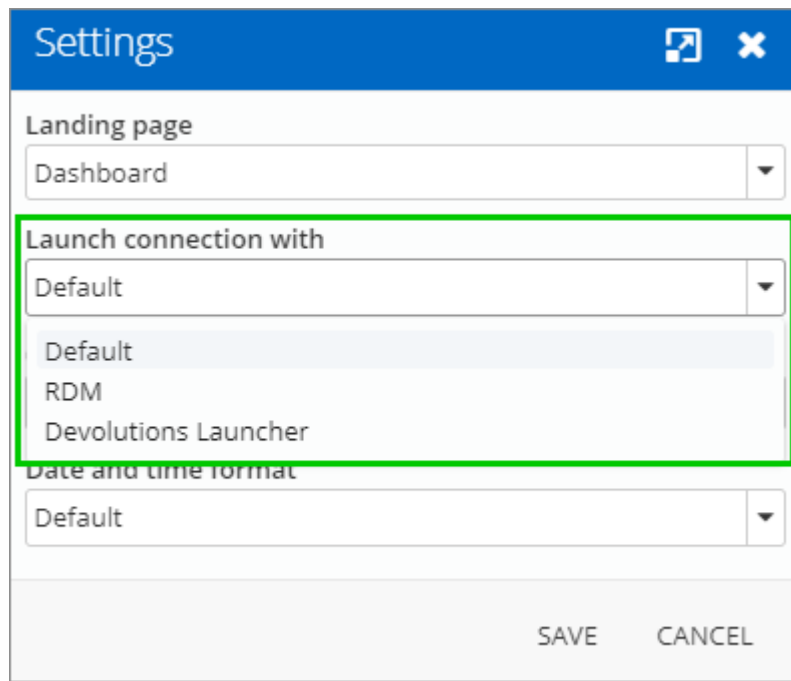
This method sets how individual users open remote connections.

1. Click the **user avatar** in the upper right corner.
2. Click **Settings**.



User Settings

3. Choose **Devolutions Launcher** from the drop-down list and **Save**.



Settings - Launch connection with Devolutions Launcher

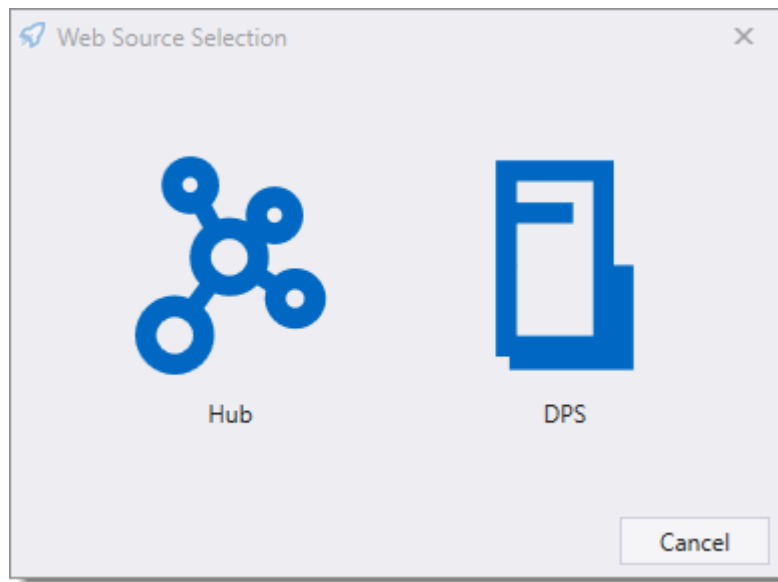
8.3.1.1 Windows

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server.



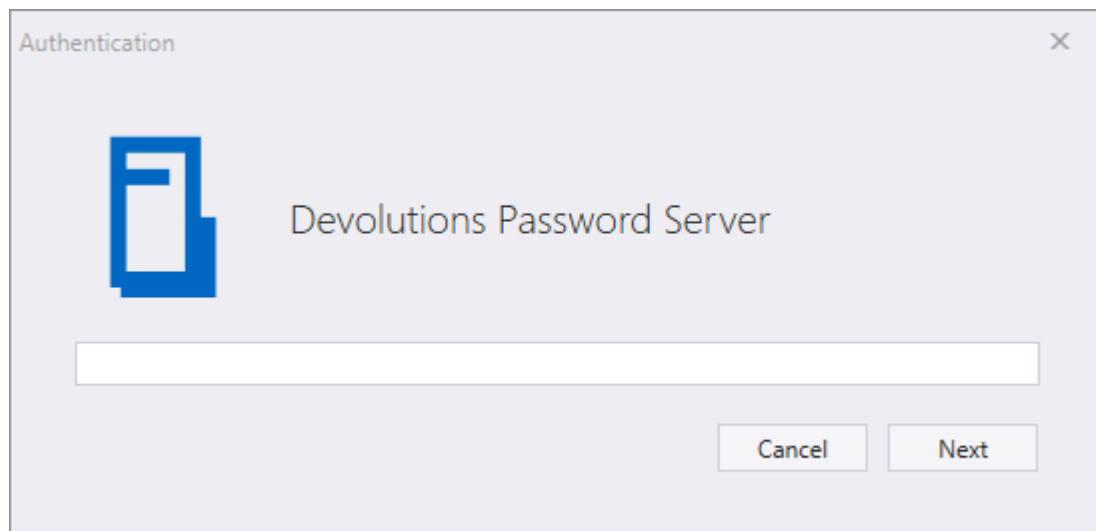
Web source login is available in the **Settings – Source** of Devolutions Launcher.

1. Choose **Devolutions Password Server**.



Choose a web source

2. Enter the Devolutions Password Server web address and click **Next**.

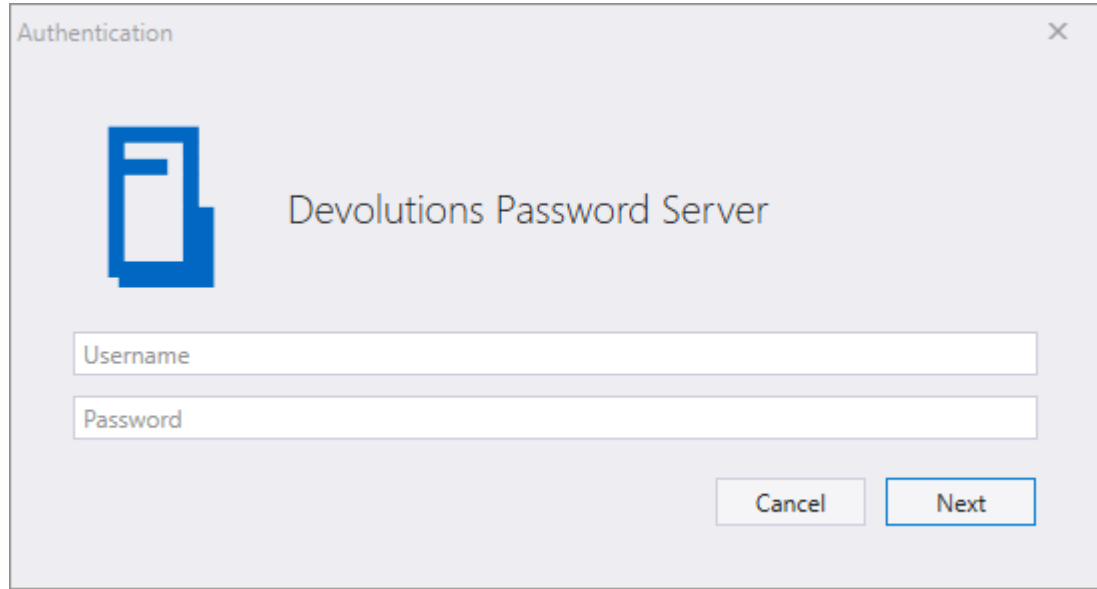


Devolutions Password Server Web Address

3. Fill in your Devolutions Password Server credentials or choose **Membership**, if available at this time, and choose between these options:
 - Domain user
 - Database user
 - Local Machine user
 - Devolutions Password Server Custom user

- Windows authentication

You can login with **Azure Active Directory** if you use it to manage your users. In Devolutions Password Server and Remote Desktop Manager this authentication type is called **Office365**.



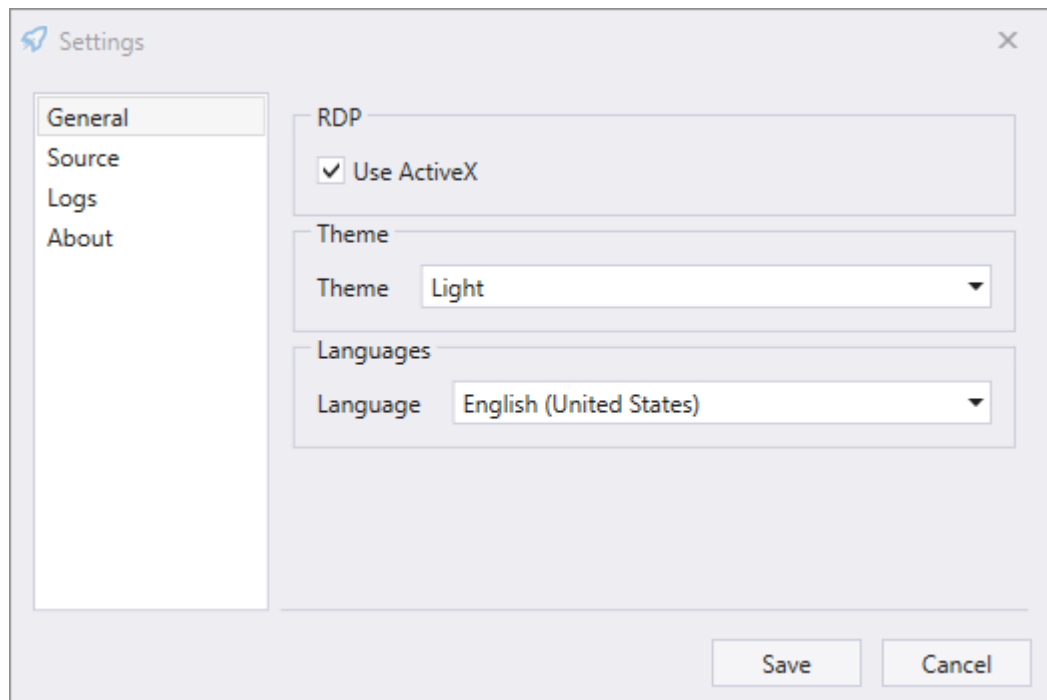
Devolutions Password Server Credentials

SETTINGS

GENERAL

In this menu you can personalize the following options:

- Use Active X to open RDP sessions. When unchecked, RDP sessions will open using FreeRDP protocol.
- Choose the color theme of Devolutions Launcher.
- Choose between the available languages. Close the application and the icon in the notification area to activate the new setting.



Devolutions Launcher Settings - General

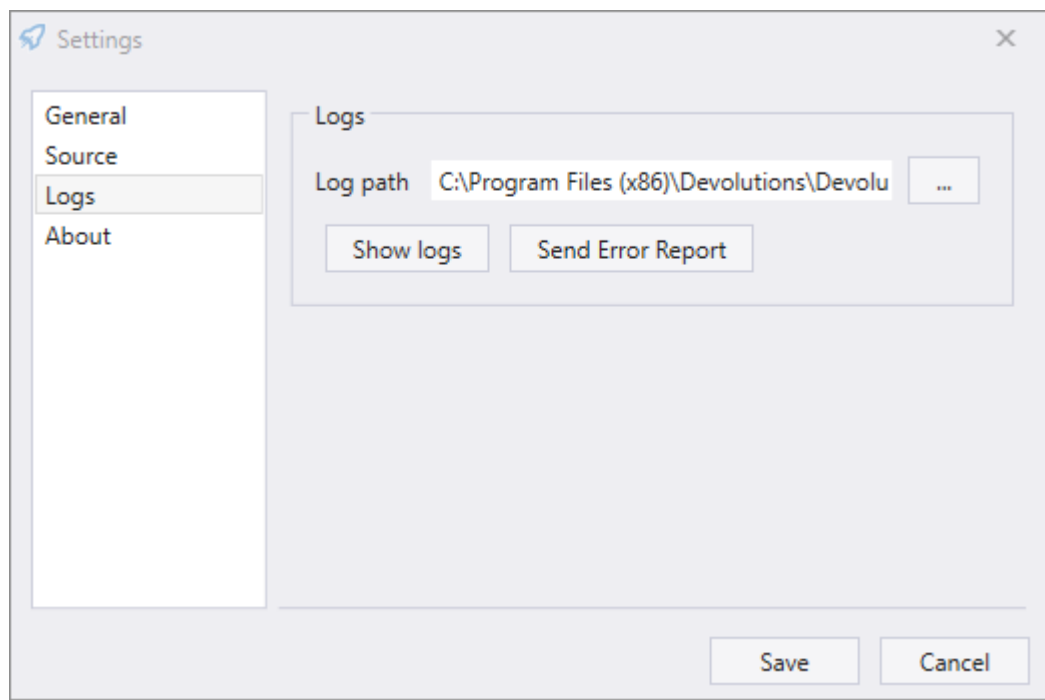
SOURCE

Log in or out of your connected source.

LOGS

The information in this section is primarily for administrators and application developers.

The log records events into a text file.



Devolutions Launcher Settings - Logs

1. Create a new log file (it can be a text document) before choosing the path.
2. Click the ellipsis button to select the path to save the log file, then save.

ABOUT

View Devolutions Launcher version and check for updates.

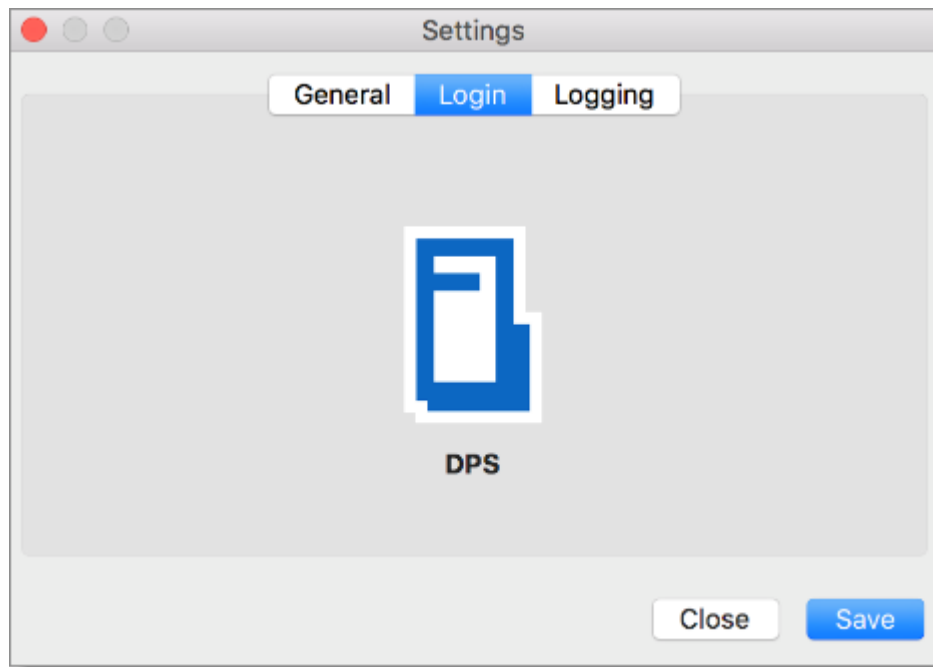
8.3.1.2 macOS

When you finish the installation of Devolutions Launcher, you are prompted to login with Devolutions Password Server.



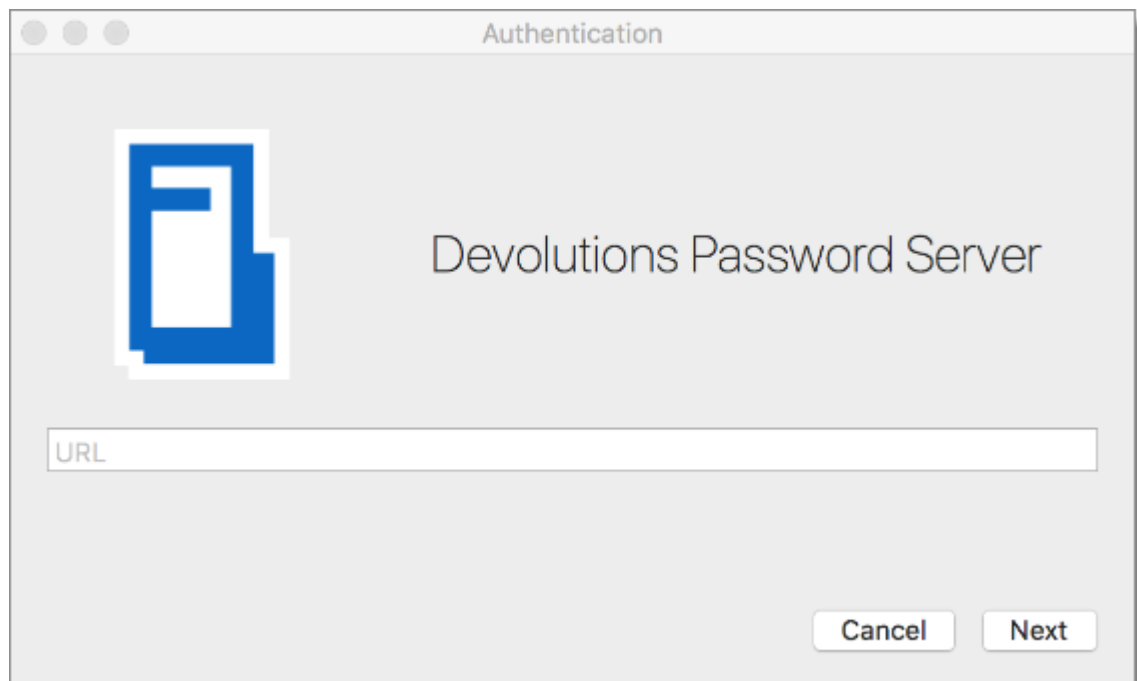
Web source login is available in the **Settings – Login** of Devolutions Launcher.

1. Click **Devolutions Password Server**.



Click Devolutions Password Server

2. Enter the Devolutions Password Server web address and click **Next**.

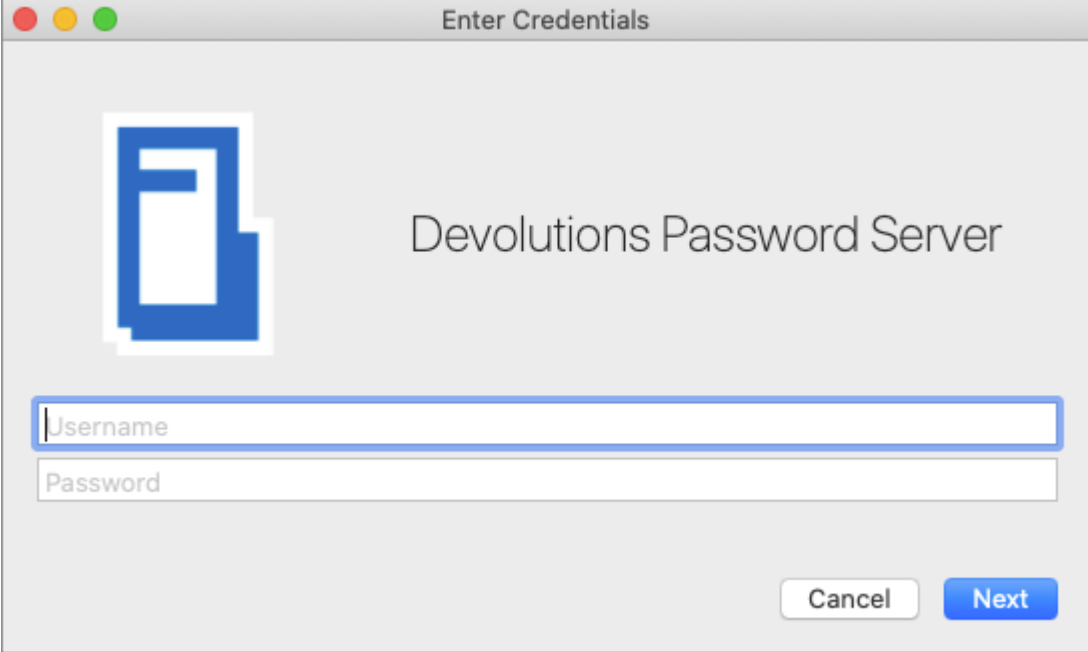


Devolutions Password Server Web Address

3. Fill in your Devolutions Password Server credentials or choose **Membership**, if available at this time, and choose between these options:

- Domain user
- Database user
- Local Machine user
- Devolutions Password Server Custom user
- Windows authentication

You can login with **Azure Active Directory** if you use it to manage your users. In Devolutions Password Server and Remote Desktop Manager this authentication type is called **Office365**..



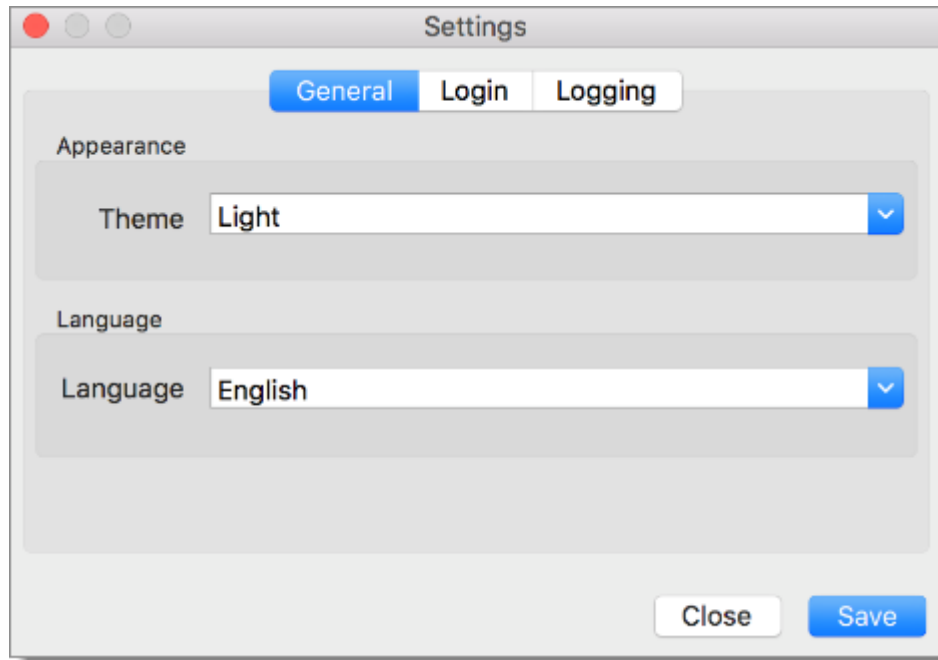
Devolutions Password Server Credentials

SETTINGS

GENERAL

In this menu you can personalize the following options:

- Choose the color theme of Devolutions Launcher.
- Choose between the available languages. Close the application to activate the new setting.



Devolutions Launcher Settings - General

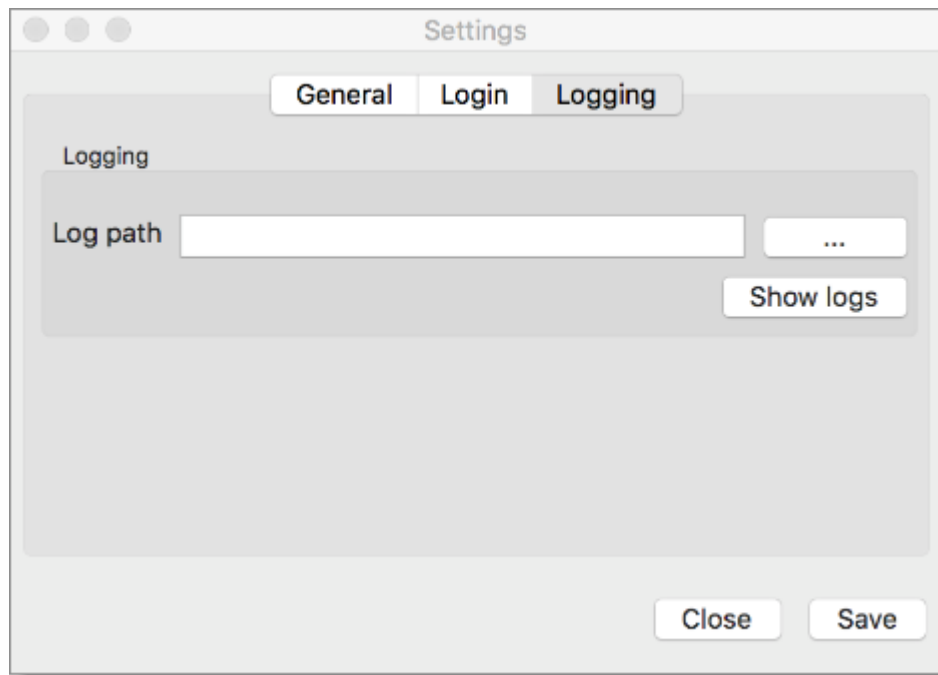
LOGIN

Log in or out of your connected source

LOGGING

The information in this section is primarily for administrators and application developers.

The log records events into a text file.

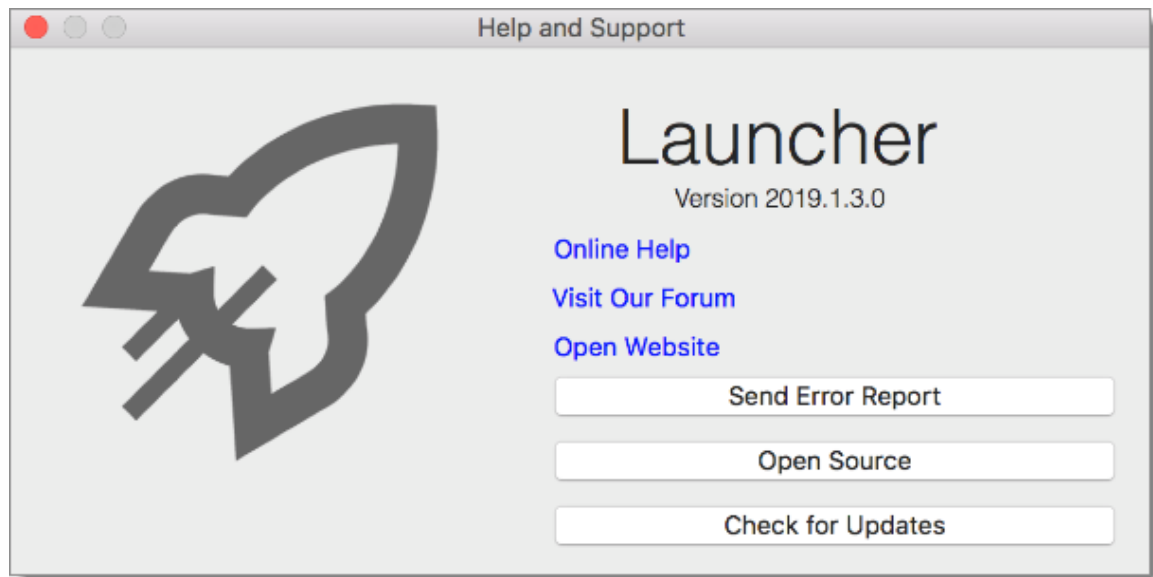


Devolutions Launcher Settings - Logs

1. Create a new log file (it can be a text document) before choosing the path.
2. Click the ellipsis button to select the path to save the log file, then save.

HELP AND SUPPORT

View Devolutions Launcher version and check for updates.



Devolutions Launcher Help and Support

8.3.1.3 Android

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server.



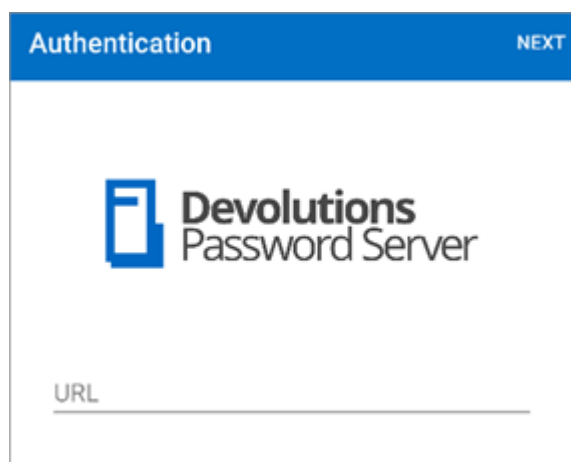
Web source login is available in the hamburger menu, then tap **Login** of Devolutions Launcher.

1. Choose **Devolutions Password Server**.



Choose a Web Source

2. Enter the Devolutions Password Server web address and tap **Next**.

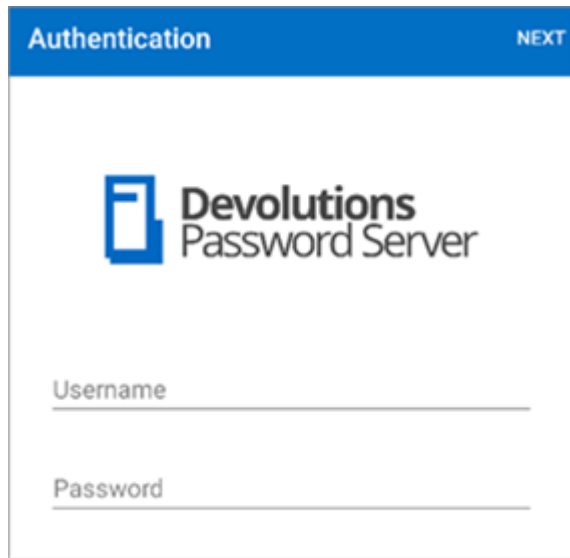


Devolutions Password Server Web Address

3. Fill in your Devolutions Password Server credentials or choose **Membership**, if available at this time, and choose between these options:

- Domain user
- Database user
- Local Machine user
- Devolutions Password Server Custom user
- Windows authentication

You can login with **Azure Active Directory** if you use it to manage your users. In Devolutions Password Server and Remote Desktop Manager this authentication type is called **Office365**.



Devolutions Password Server Credentials



Secure the application with a password in the hamburger menu, **Security**. Once registered, there is no way to recover the password.

DEVOLUTIONS LAUNCHER MENU

Click the hamburger button in the top left corner to access Devolutions Launcher menu.

LOG OUT

Log out of Devolutions Launcher application.

SETTINGS

Set all the settings related to your Devolutions Launcher:

- Theme: Change the color theme of the application.
- Security: Application password, Background lock, Fingerprint activation, Lock application.
- Language: Choose between the available languages. An application relaunch is necessary.
- Sessions: Full-screen options.
- RDP: Screen size, Enabling logging and redirection.
- Terminal: Set terminal appearance.
- User interface: Pointer size mode in session.
- Help: Reset help messages.
- Application: Logs and about Devolutions Launcher.

OPEN DPS

Open a session by tapping **Open DPS**.

HELP AND SUPPORT

Find all the support links and help with the application.

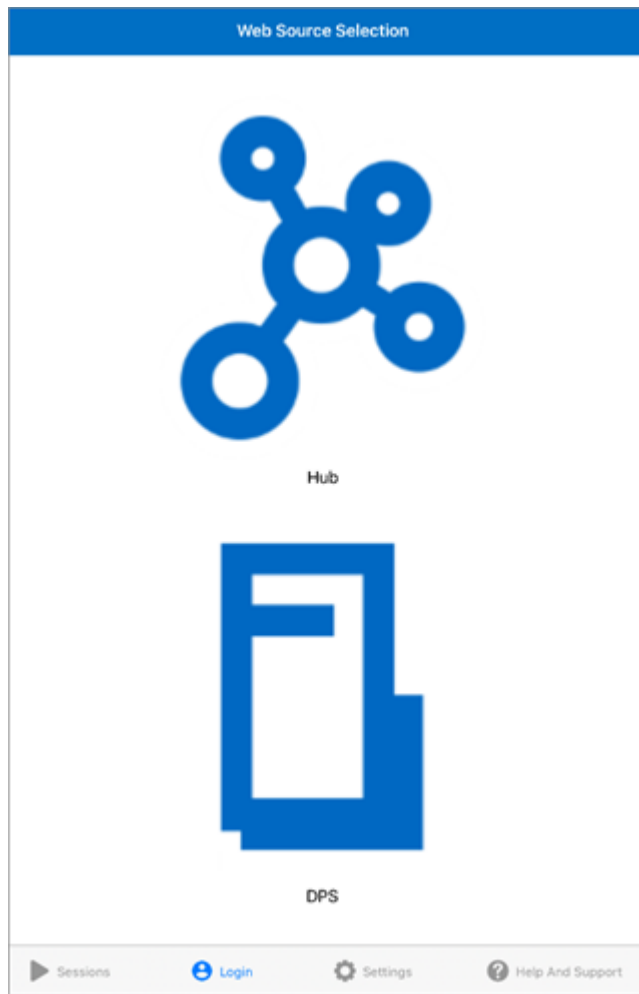
8.3.1.4 iOS

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server..



Web source login is available in the **Login** of Devolutions Launcher.

1. Choose **Devolutions Password Server**.



Devolutions Launcher Web Source Selection

2. Enter the Devolutions Password Server web address and tap **Next**.



Devolutions Password Server Web Address

3. Fill in your Devolutions Password Server credentials or choose **Membership**, if available at this time, and choose between these options:
- Domain user
 - Database user
 - Local Machine user
 - Devolutions Password Server Custom user
 - Windows authentication

You can login with **Azure Active Directory** if you use it to manage your users. In Devolutions Password Server and Remote Desktop Manager this authentication type is called **Office365**.

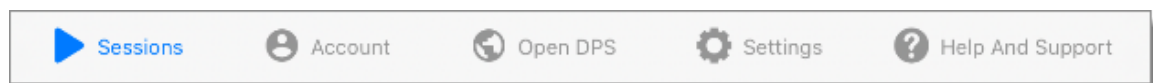
The screenshot shows the 'Authentication' window of the Devolutions Password Server. At the top, there is a blue header bar with three navigation links: '< Web Source Selection', 'Authentication', and 'Next'. Below the header, the Devolutions logo (a blue square with a white stylized 'D') is positioned to the left of the text 'Devolutions Password Server'. Underneath the logo, there are two input fields: 'Username' and 'Password'. At the bottom of the window, there is a light gray bar containing four icons with corresponding labels: a play button for 'Sessions', a blue circle with a white 'i' for 'Login', a gear for 'Settings', and a question mark for 'Help And Support'.

Remote Desktop Manager Credentials



Secure the application with a password in **Settings - Security**. Once registered, there is no way to recover the password.

DEVOLUTIONS LAUNCHER MENU



Devolutions Launcher Menu

SESSIONS

View the open sessions

ACCOUNT

Log in or out of your connected source

OPEN DPS

Open a session by tapping ***Open DPS***.

SETTINGS

Set all the settings related to your Devolutions Launcher:

- Security: Application password, Background lock, Touch ID activation, Lock application.
- Language: Choose between the available languages. An application relaunch is necessary.
- Sessions: Full-screen option.
- RDP: Screen size, Enabling logging and redirection.
- Terminal: Set terminal appearance.
- User interface: Pointer size mode in session.
- Application: Logs and about Devolutions Launcher.

HELP AND SUPPORT

Find all the support links and help with the application.

8.3.2 Devolutions Password Hub

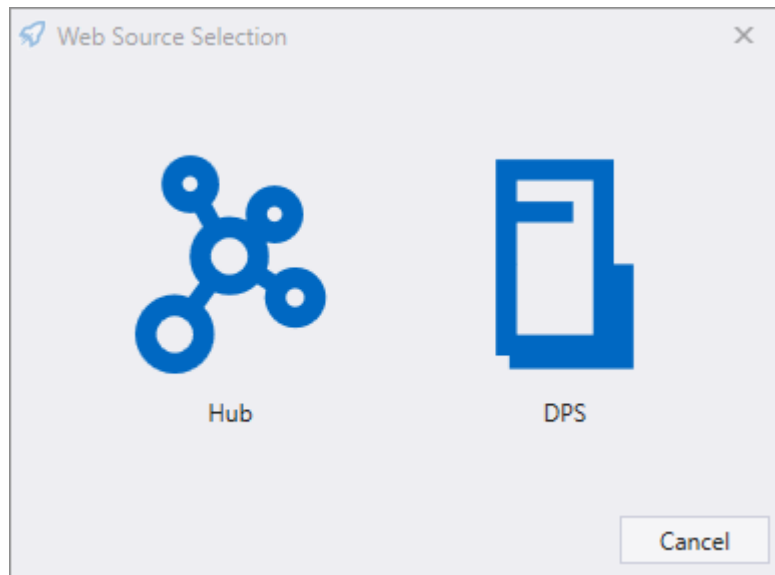
8.3.2.1 Windows

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server.



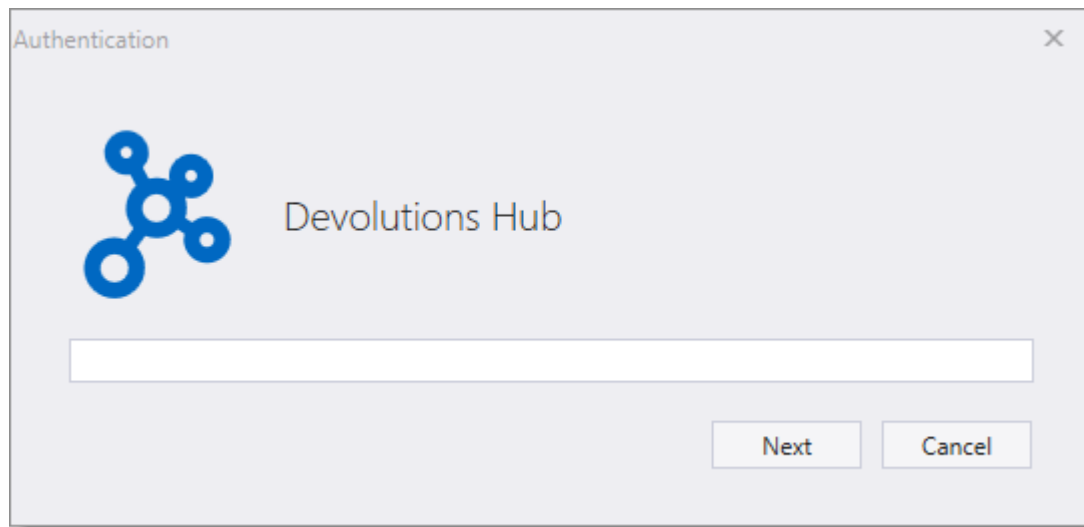
Web source login is available in the **Settings – Source** of Devolutions Launcher.

1. Choose **Devolutions Password Hub**.



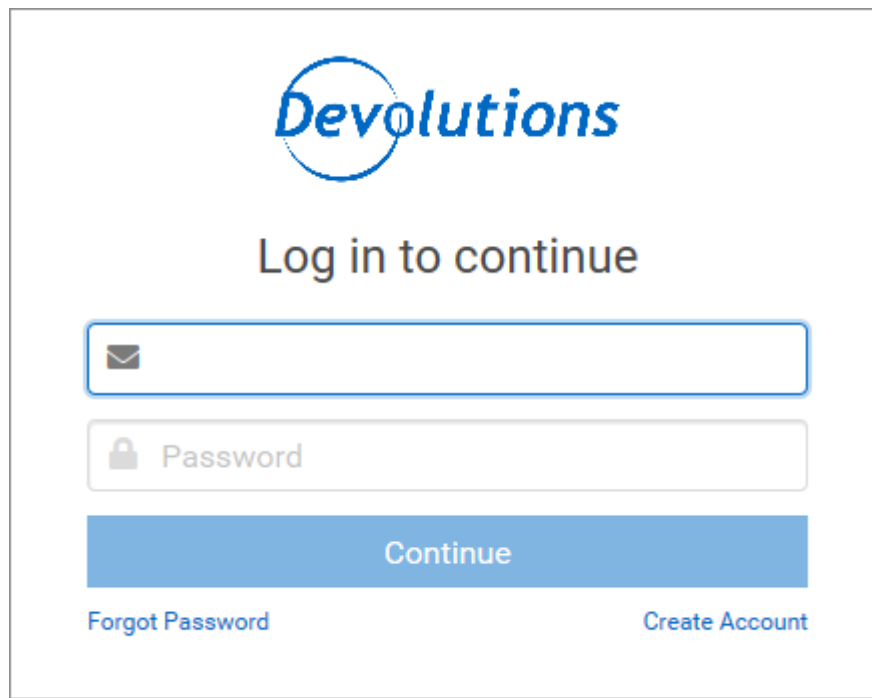
Choose a web source

2. Enter the Devolutions Password Hub web address and click **Next**.



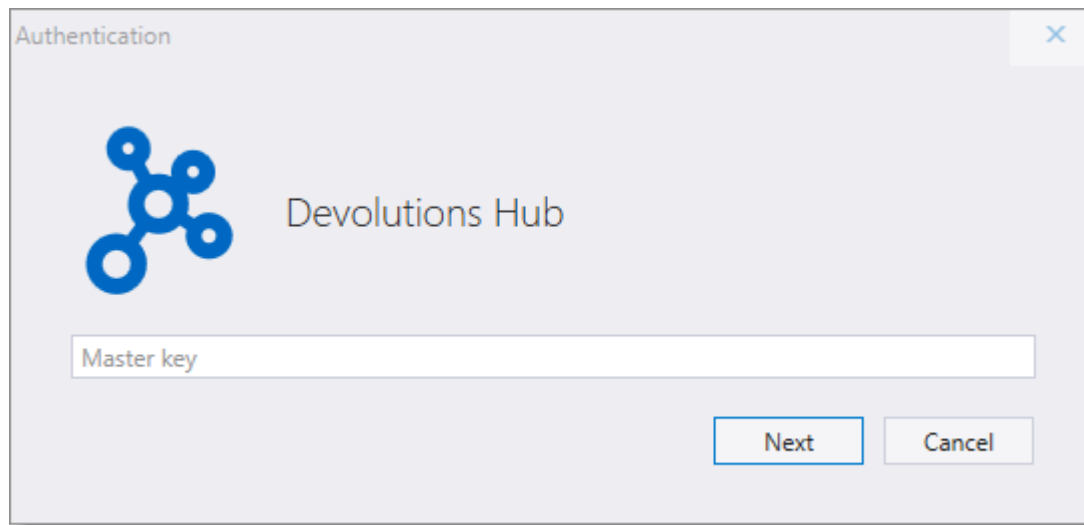
Devolutions Password Hub Web Address

3. Fill with your Devolutions Password Hub credentials and **Continue**.



Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub masterkey and click **Next**.



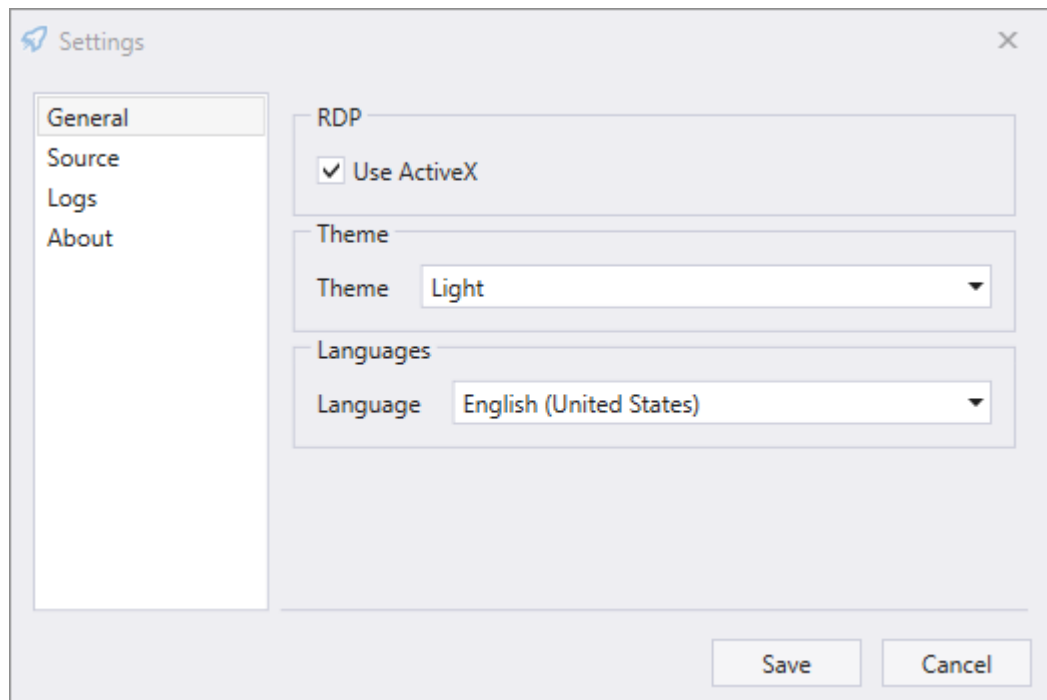
Devolutions Password Hub Master Key

SETTINGS

GENERAL

In this menu you can personalize the following options:

- Use Active X to open RDP sessions. When unchecked, RDP sessions will open using FreeRDP protocol.
- Choose the color theme of Devolutions Launcher.
- Choose between the available languages. Close the application and the icon in the notification area to activate the new setting.



Devolutions Launcher Settings - General

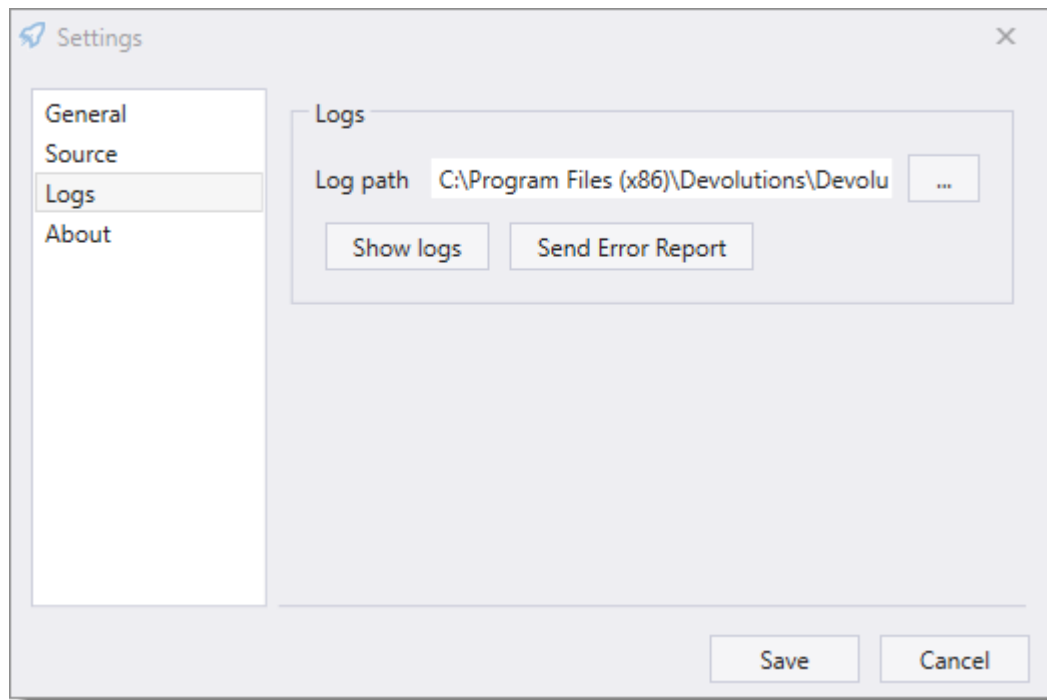
SOURCE

Log in or out of your connected source.

LOGS

The information in this section is primarily for administrators and application developers.

The log records events into a text file.



Devolutions Launcher Settings - Logs

1. Create a new log file (it can be a text document) before choosing the path.
2. Click the ellipsis button to select the path to save the log file, then save.

ABOUT

View Devolutions Launcher version and check for updates.

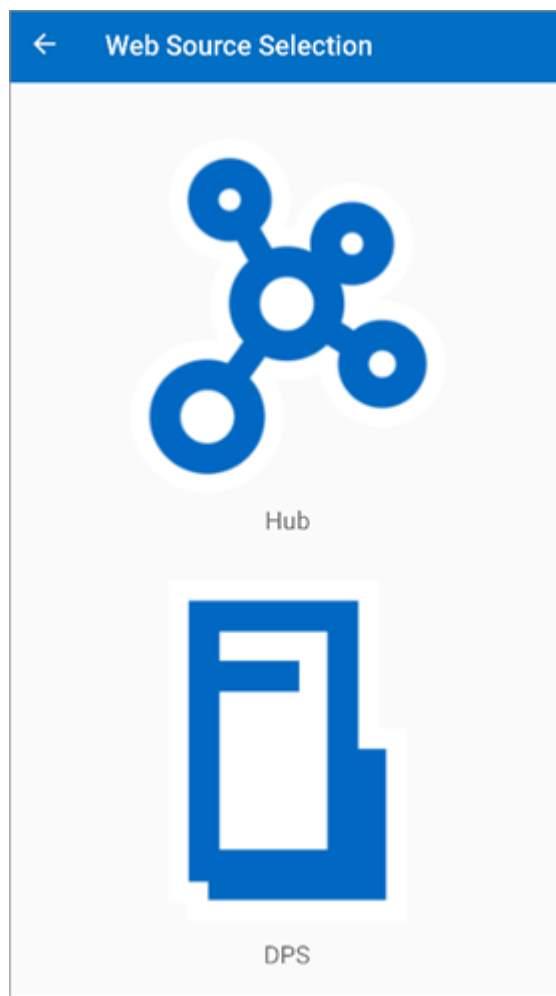
8.3.2.2 Android

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server.



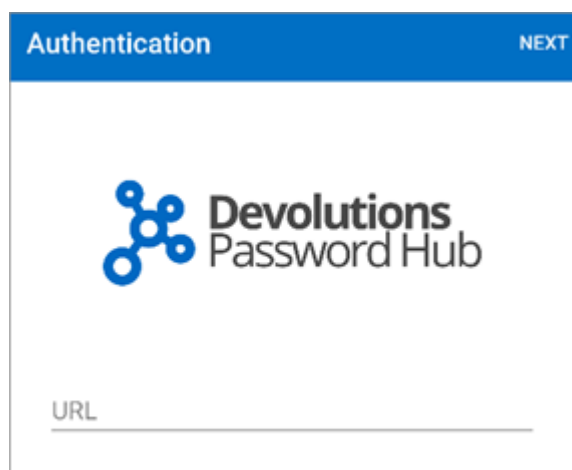
Web source login is available in the hamburger menu, then tap **Login** of Devolutions Launcher.

1. Choose **Devolutions Password Hub**.



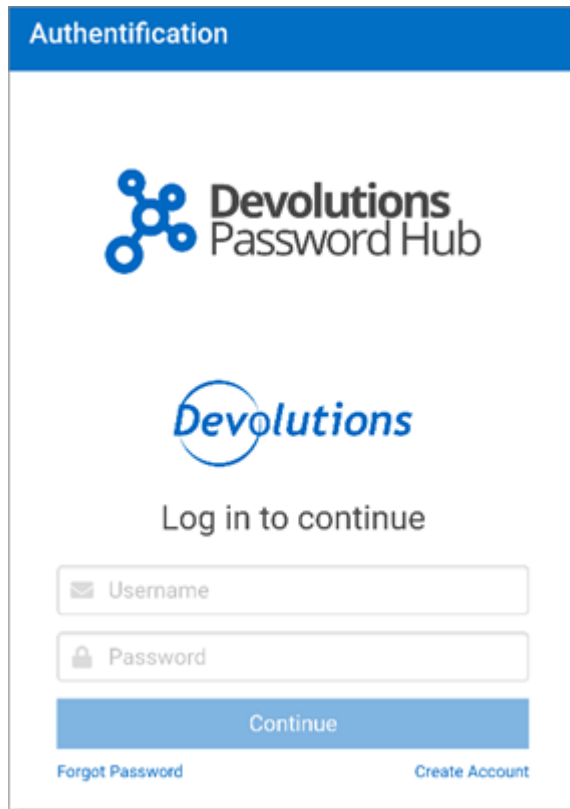
Choose a Web Source

2. Enter the Devolutions Password Hub web address and tap **Next**.



Devolutions Password Hub Web Address

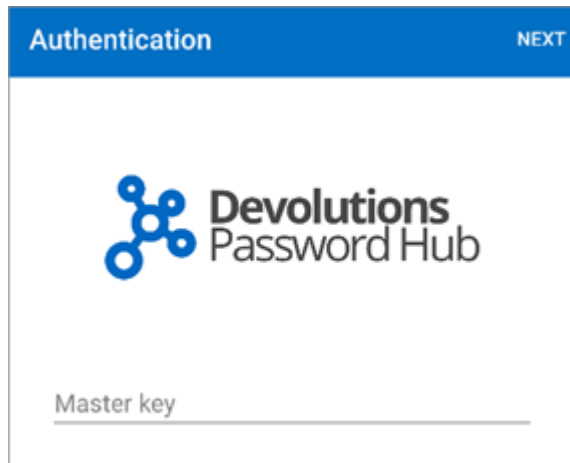
3. Fill with your Devolutions Password Hub credentials and **Continue**.



The image shows the 'Authentication' screen of the Devolutions Password Hub. At the top, there is a blue header with the word 'Authentication' in white. Below the header, the Devolutions Password Hub logo is displayed, consisting of a blue icon of three interconnected circles and the text 'Devolutions Password Hub'. Underneath the logo, the word 'Devolutions' is written in a blue, stylized font. Below this, the text 'Log in to continue' is centered. There are two input fields: the first is labeled 'Username' with an envelope icon, and the second is labeled 'Password' with a lock icon. Below these fields is a blue button labeled 'Continue'. At the bottom of the screen, there are two links: 'Forgot Password' on the left and 'Create Account' on the right.

Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub Master key and click **Next**.



The image shows the 'Authentication' screen of the Devolutions Password Hub, similar to the previous one, but with a 'NEXT' button in the top right corner of the blue header. The 'Username' and 'Password' fields are not present. Instead, there is a single input field labeled 'Master key' with a key icon. The Devolutions Password Hub logo and the word 'Devolutions' are still present.

Devolutions Password Hub Master Key

DEVOLUTIONS LAUNCHER MENU

Click the hamburger button in the top left corner to access Devolutions Launcher menu.

LOG OUT

Log out of Devolutions Launcher application.

SETTINGS

Set all the settings related to your Devolutions Launcher:

- Theme: Change the color theme of the application.
- Security: Application password, Background lock, Fingerprint activation, Lock application.
- Language: Choose between the available languages. An application relaunch is necessary.
- Sessions: Full-screen options.
- RDP: Screen size, Enabling logging and redirection.
- Terminal: Set terminal appearance.
- User interface: Pointer size mode in session.
- Help: Reset help messages.
- Application: Logs and about Devolutions Launcher.

OPEN HUB

Open a session by tapping **Open Hub**.

HELP AND SUPPORT

Find all the support links and help with the application.

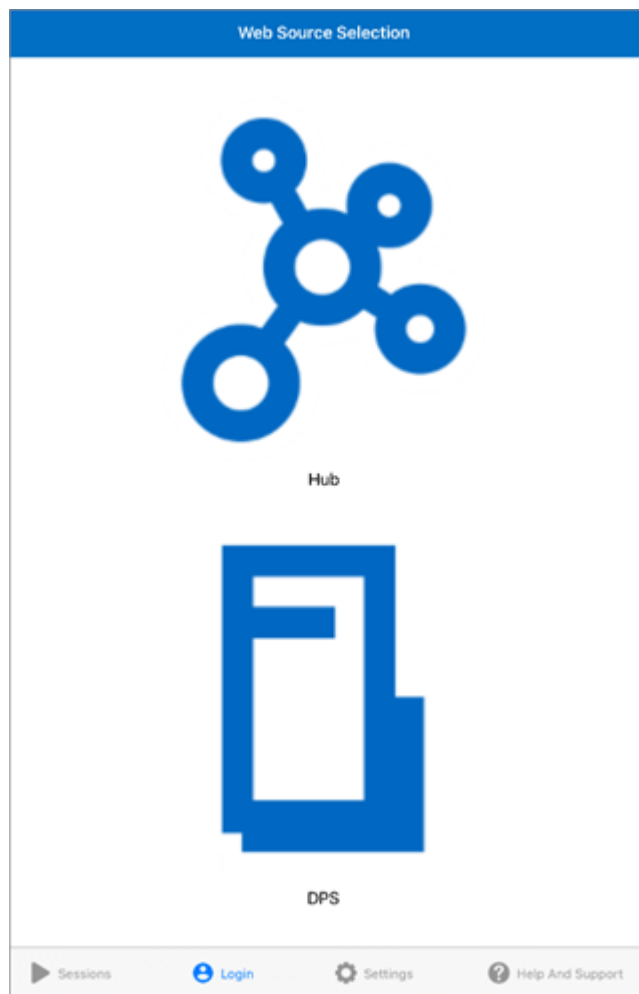
8.3.2.3 iOS

When you finish the installation of Devolutions Launcher, you are prompted to choose a web source between Devolutions Password Hub and Devolutions Password Server..



Web source login is available in the **Login** of Devolutions Launcher.

1. Choose **Devolutions Password Hub**.



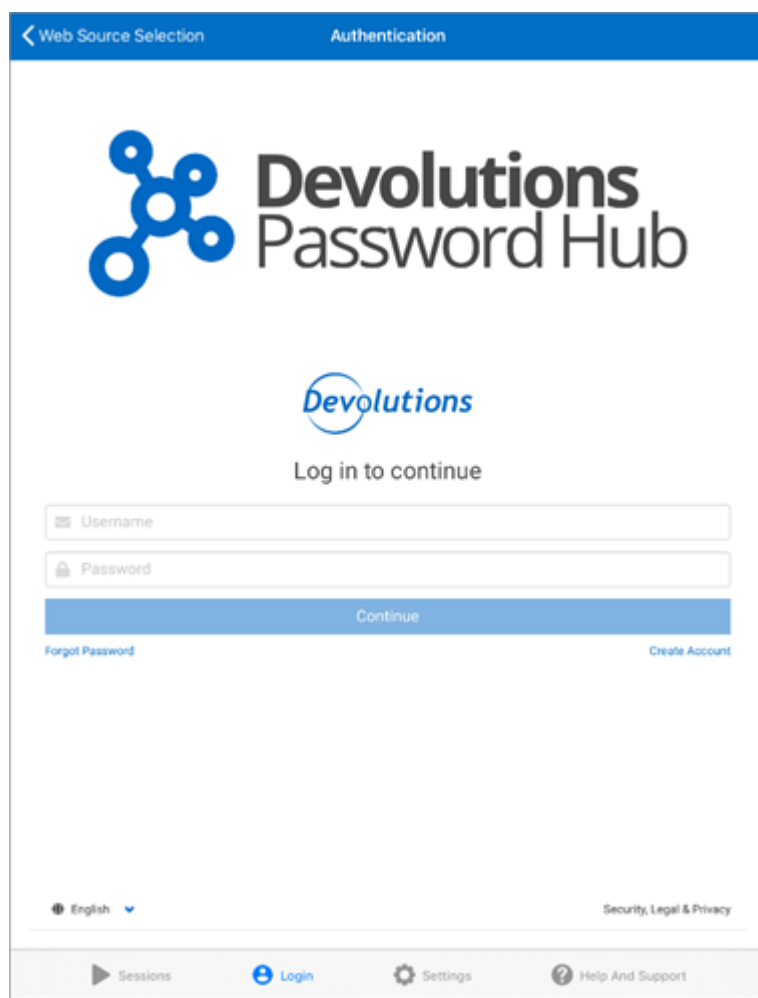
Devolutions Launcher Web Source Selection

2. Enter the Devolutions Password Hub Web address and tap **Next**.



Devolutions Password Hub Web Address

3. Fill with your Devolutions Password Hub credentials and ***Continue***.



The screenshot shows the 'Authentication' page of the Devolutions Password Hub. At the top, there is a blue header bar with a back arrow and the text 'Web Source Selection' on the left, and 'Authentication' on the right. Below the header, the Devolutions Password Hub logo is displayed, consisting of a blue icon of four interconnected circles and the text 'Devolutions Password Hub'. Underneath the logo is the Devolutions logo in blue. The text 'Log in to continue' is centered. Below this, there are two input fields: 'Username' and 'Password'. A blue 'Continue' button is positioned below the password field. At the bottom of the login section, there are two links: 'Forgot Password' on the left and 'Create Account' on the right. At the very bottom of the page, there is a footer bar with a language selector set to 'English' and a link to 'Security, Legal & Privacy'. A navigation bar at the bottom contains icons and labels for 'Sessions', 'Login' (highlighted in blue), 'Settings', and 'Help And Support'.

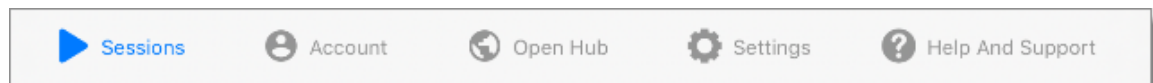
Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub Master key and click **Next**.



Devolutions Password Hub Master Key

DEVOLUTIONS LAUNCHER MENU



Devolutions Launcher Menu

SESSIONS

View the open sessions

ACCOUNT

Log in or out of your connected source

OPEN HUB

Open a session by tapping ***Open Hub***.

SETTINGS

Set all the settings related to your Devolutions Launcher:

- Security: Application password, Background lock, Touch ID activation, Lock application.
- Language: Choose between the available languages. An application relaunch is necessary.
- Sessions: Full-screen option.
- RDP: Screen size, Enabling logging and redirection.
- Terminal: Set terminal appearance.
- User interface: Pointer size mode in session.
- Application: Logs and about Devolutions Launcher.

HELP AND SUPPORT

Find all the support links and help with the application.

8.4 Utilization

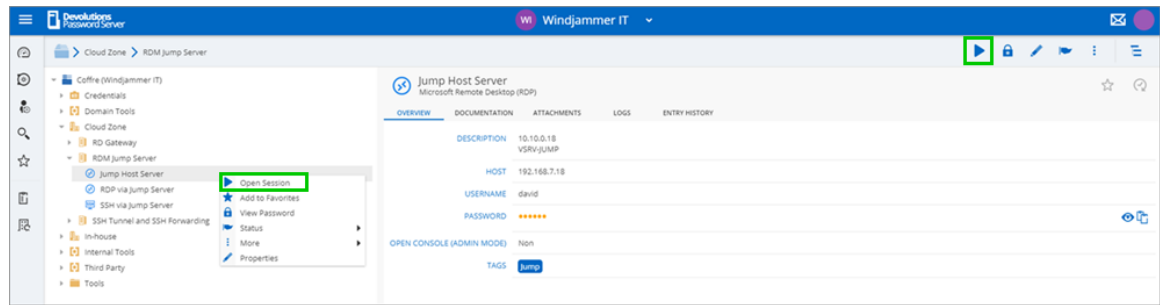
8.4.1 Windows and macOS

HOW TO OPEN REMOTE CONNECTIONS WITH DEVOLUTIONS LAUNCHER

An overview of *Devolutions Launcher*

OPEN A SESSION WITH DEVOLUTIONS PASSWORD SERVER

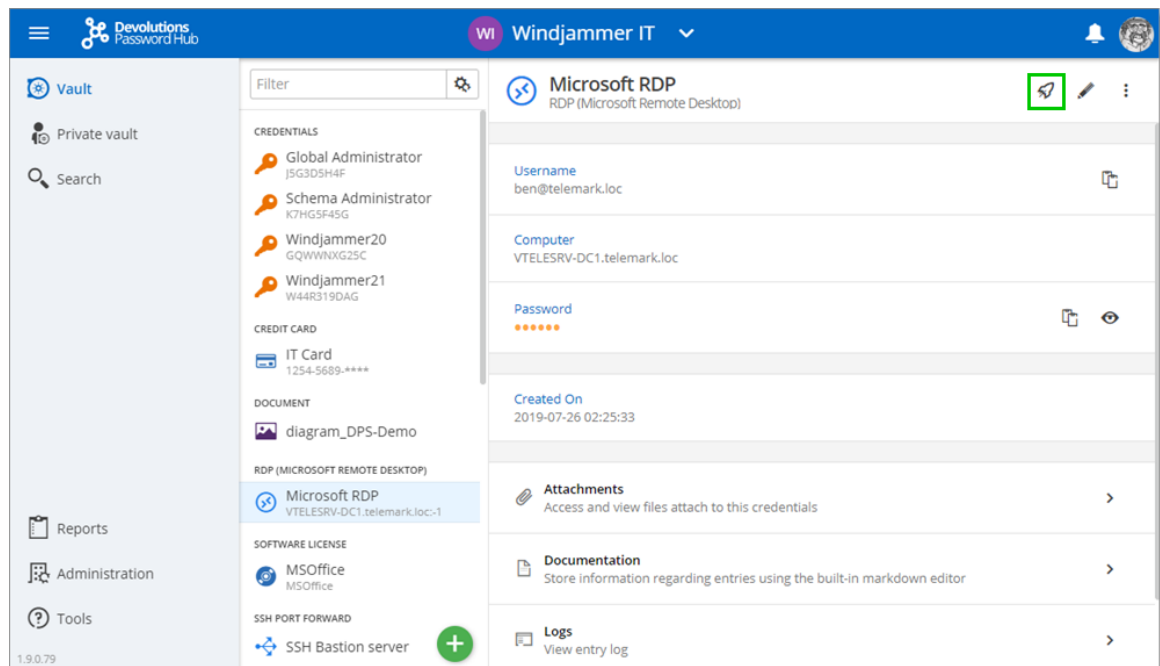
Click the play button  or open a session in the right-click contextual menu.



Open a Devolutions Password Server session

OPEN A SESSION WITH DEVOLUTIONS PASSWORD HUB

Click the *Devolutions Launcher* icon.



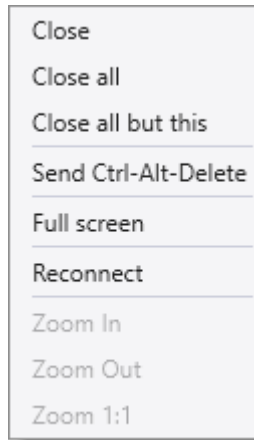
Open a Devolutions Password Hub session

SESSION SETTINGS IN DEVOLUTIONS LAUNCHER

Undock or float a session by clicking and holding the tab away from the window and releasing it.

Re dock it by clicking and holding the tab, releasing it on the upper part of Devolutions Launcher.

To use the shortcut **Ctrl-Alt-Delete** in a session, right-click on the session tab to open the menu and click on the **Send Ctrl-Alt-Delete** button.



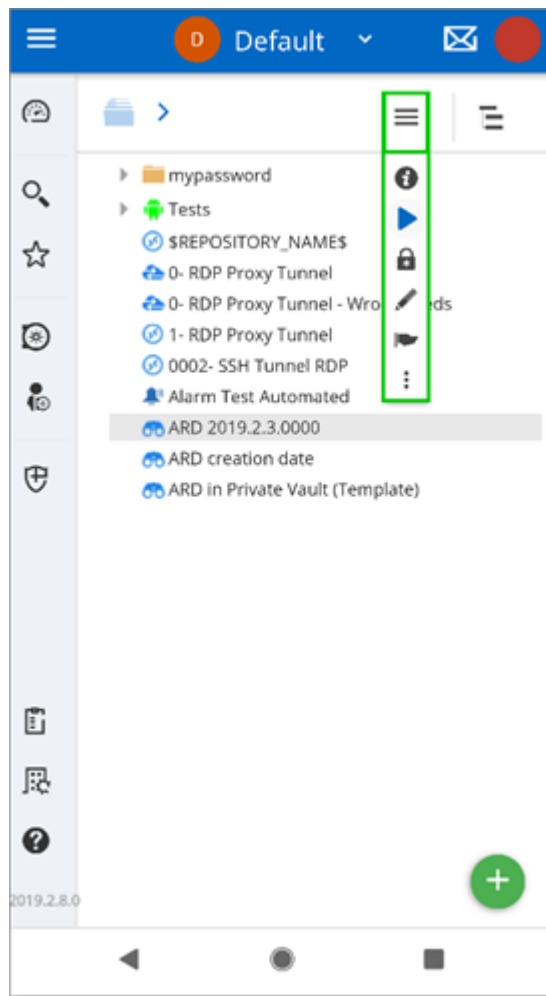
Session Settings

8.4.2 Android and iOS

OPEN A SESSION WITH ANDROID AND IOS FROM DEVOLUTIONS PASSWORD SERVER

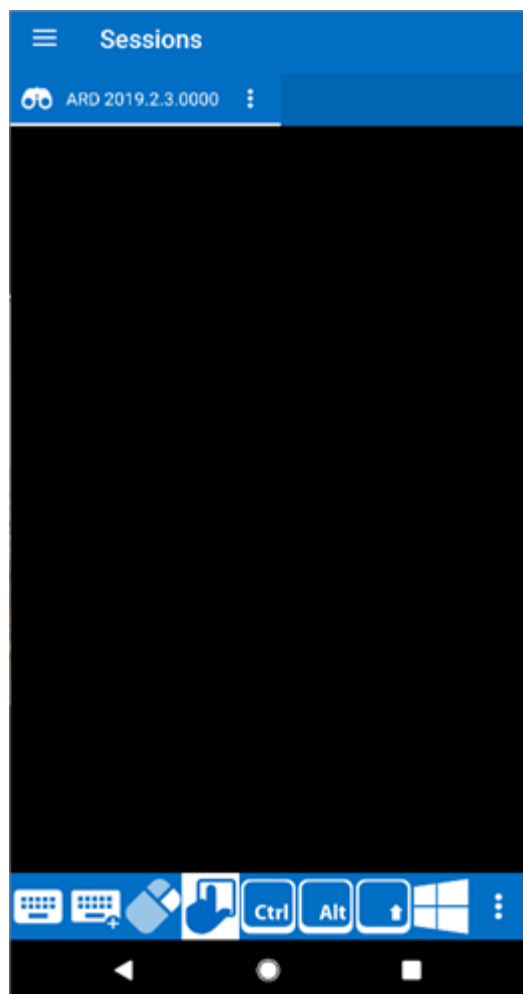
If the hamburger menu is hidden, in the **Vault** section, follow these steps to launch a session:

1. Click on a session in Devolutions Password Server from your Android or iOS device.
2. Close it to go back to the vault view.
3. Press on the hamburger menu at the top right corner than the play button ▶ to launch the session.



Android Hamburger Menu

Your remote connection opens in Devolutions Launcher.



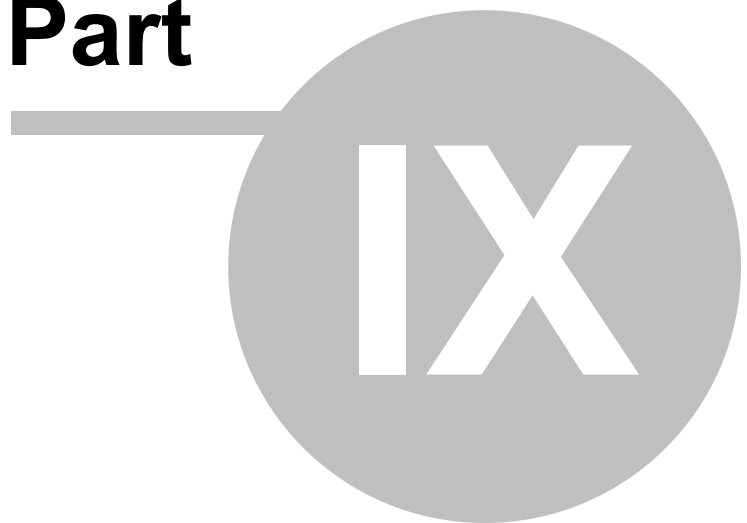
Android Sessions

The bottom menu allows to show or hide the keyboard, perform a right-click or move the cursor of the remote connection with the touch interface of your device.

Shortcut keys are displayed and other features are available in the hidden menu.

Support/Resources

Part



9 Support/Resources

9.1 FAQ (Frequently Asked Questions)

WHAT IS DEVOLUTIONS SERVER?

Devolutions Server is a specialized data source for our various client applications of the **Remote Desktop Manager** platform.

WHY BUY DEVOLUTIONS SERVER?

Ideal for businesses that would prefer to store their data in-house, want to deploy their own SSL certificate or firewall or who need Active Directory integration with role management.

WHAT ARE THE KEY BENEFITS OF DEVOLUTIONS SERVER?

Devolutions Server is installed on your hardware, in your environment, or with your ISP to give you total control of everything, including:

- Active Directory integration
- Role management
- Hardware
- Operating System
- Firewall / Application Delivery
- Load Balancing / Fault tolerant environment for the web server layer.
- Database, including clustering / failover capabilities.
- Backups
- SSL certificates

Devolutions Server also offers an improved security model, as database access is limited to the server and no direct connection is established. This secure architecture is a significant improvement over standard client-server architecture. (SQL Server data source)

CAN I GET A TRIAL OF DEVOLUTIONS SERVER?

Yes - [Request a trial](#)

DOES DEVOLUTIONS SERVER INCLUDE A CLIENT LICENSE OF REMOTE DESKTOP MANAGER?

Devolutions Server does not include any client licenses.

IS DEVOLUTIONS SERVER SUBSCRIPTION BASED?

Yes, Devolutions Server is subscription based. You can subscribe for one (1) year or three (3) years at a time. Giving you unlimited client connectivity for that period of time.

WHAT IF I NO LONGER WANT/NEED A DEVOLUTIONS SERVER? IS MY DATA STILL ACCESSIBLE?

Yes, once your Devolutions Server subscription is expired you can still access the data using one of our applications. However the Devolutions Server data source will no longer be accessible. You will need to reconfigure your clients to connect directly to the database using a SQL Server data source. Since Active Directory integration will not be allowed anymore, you will need to reassign user permissions.

CAN I UPGRADE FROM A SQL SERVER DATA SOURCE TO DEVOLUTIONS SERVER?

Yes, the underlying SQL server database structure for the SQL Server data source is a subset of the Devolutions Server database structure. When installing/configuring the Devolutions Server simply specify the existing database and choose upgrade.

Note: Before executing any database modification it is always a good idea to make sure you have a proper backup of the database.

CAN I DOWNGRADE FROM A DEVOLUTIONS SERVER DOWN TO SQL SERVER DATA SOURCE?

Yes, since the database for Devolutions Server is a superset of the SQL Server data source. Simply connect to the database using the SQL Server data source and your sessions will all be available. Keep in mind that not all Devolutions Server features will be accessible when using the SQL Server data source, you will need to review all security permissions.

9.2 Previous Versions

DESCRIPTION

Here are the links to the pdf manuals of past releases.

[Devolutions Server 4.6](#)

[Devolutions Server 4.5](#)

[Devolutions Server 4.0](#)

[Devolutions Server 3.2](#)

[Devolutions Server 3.0](#)

[Devolutions Server 2.5](#)

9.3 Technical Support

Hours: Monday to Friday 7:30 a.m. to 6:00 p.m. EST

Knowledge Base: Find helpful information's and procedures regarding our [products](#).

Email: ticket@devolutions.net

Forum: <https://forum.devolutions.net/>

Language: English-Français-Deutsch

Phone: +1 844 463.0419

EXTENDED AND PREMIUM SUPPORT PLANS

Subscribers of a paid support plan receive an email address and a plan ID. You should send your support requests to the appropriate email address and provide your plan ID in the subject line.

Please consult our [Support Policy](#) for more information.





Contact Us

For any questions, feel free to contact us:

Support: ticket@devolutions.net

Phone: +1 844 463.0419

Monday to Friday 7:30 a.m. to 6 p.m. EST

Head Office

Devolutions inc.

1000 Notre-Dame

Lavaltrie, QC J5T 1M1

Canada