

Self-Hosted Repository & Management Platform

User Manual 2020.1





Table of Contents

Part I	Overview	9
1	What is Devolutions Password Server?	10
2	System Requirements	12
3	Topologies	
4	Fault Tolerance	
Part II	Getting Started	21
1	Security Checklist	23
	LDAP over SSL	
	Encrypting Connections to SQL Server	
2	Team Edition	
Part III	Installation	27
1	Installing Web Roles Prerequisites	29
2	Database Instance	
	On-Premise	
	Microsoft Azure SQL	
3	Create Devolutions Password Server instance	
4	Upgrading Devolutions Password Server	49
Part IV	Management	57
Part IV	Management Devolutions Password Server Console	57
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings	57
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General	57
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database	57 58
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authoritaging	57 58 60 61 64
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain	57 58 60 60 61 64 66 68
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365	57 58 60 60 61 64 66 68 72
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS	57 58 60 60 61 64 66 68 72 75
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced	57 58 60 60 61 64 66 68 72 75 77
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands	57 58 60 60 61 64 66 68 72 75 77 78
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users	57 58 60 60 61 64 66 68 72 75 77 78 80
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager	57 58 60 60 61 64 66 68 72 75 77 78 80 80 81 80 81 80 81 80 81 80 80 81 80 81 80 80 80 80 80 80 80 80
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced	57 58 60 60 60 61 64 66 68 72 75 77 78 80 81 82
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced View logs	57 58 60 60 61 64 66 68 72 75 77 78 80 81 82 85 87
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced View logs Explore content of website directory	57 58 60 60 61 64 66 68 72 75 77 78 80 81 82 85 87 88
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced View logs Explore content of w ebsite directory Pack Data Source	57 58 60 60 60 61 64 66 68 72 75 77 78 80 81 82 85 87 88 88 88
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced View logs Explore content of website directory Pack Data Source Options	57 58 60 60 61 64 66 68 72 75 77 78 80 81 82 85 87 88 88 91
Part IV	Management Devolutions Password Server Console Devolutions Password Server Settings General Database Advanced Settings Authentication Domain Office365 IIS Advanced Commands Import Users Backup Manager Database Advanced View logs Explore content of w ebsite directory Pack Data Source Options Advanced	57 58 60 60 61 64 66 68 72 75 77 78 80 81 82 85 87 88 88 91 92

	Database Diagnostic	
	Send Diagnostic to Support	
	View Installation Logs	
	Open Backup Folder	
	Manage Encryption Keys	
	Check for Updates	
	About	
2	Authentication	107
3	Security	109
	User Management	
	Role Management	
	Legacy properties	
	Vault Management	

Part V Web Interface

135

2 Account Menu 138 3 Vaults 144 My Vault (Private) 144 Create a New Entry 155 RDP (Mcrosoft Remote Desktop) 153 Apple Remote Desktop (ARD) 171 Information 176 Alarm Codes 177 Email Account 179 Website 188 Note/Secure Note 188 Contact 189 Document 191 Folder 194 Credential Entry 196 Connection String 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 207 Inport 207 4 Reports 215 Dagnostic 215 Dagnostic 215 Dagnostic 216 Security Management 222 Users 223 General 224 Information 226 Tono Factor 2	1	Dashboard	
3 Vaults 146 My Vault (Private) 144 Create a New Entry 155 Session 153 RDP (Microsoft Remote Desktop) 153 Apple Remote Desktop (ARD) 171 Information 176 Alarro Codes 177 Email Account 179 Website 188 Note/Secure Note 188 Contact 189 Document. 191 Folder 194 Credential Entry 196 Connection String. 197 One-Time Passw ord (OTP). 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 215 Dagnostic 219 Scheduling Reports 215 Dagnostic 216 Scheduling Reports 223 General 224 Information 225 Quitt Anangement 222 Security Management	2	Account Menu-	
My Vault (Private) 144 Create a New Entry 155 Create a New Entry 155 Create a New Entry 153 ADple Remote Desktop (ARD) 171 Information 176 Alarm Codes 177 Email Account 176 Note/Secure Note 188 Contact 189 Document. 191 Folder 194 Credential Entry. 196 Connection String. 197 One-Time Password (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord. 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 223 General 224 Information 225 Train Stration 226 Tow Factor 227 Roles <th>3</th> <th>Vaulte</th> <th></th>	3	Vaulte	
my value (Frivate) 144 Create a New Entry 155 RDP (Mcrosoft Remote Desktop) 153 Apple Remote Desktop (ARD) 171 Information 176 Alarm Codes 177 Enail Account 179 Website 186 Note/Secure Note 188 Contact 189 Document 191 Folder 194 Credential Entry 196 Connection String 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 215 Dagostic 215 Dagostic 215 Dagostic 215 Users 223 General 224 Information 225 Querty Management 222 Users 223 General 224 Information 225 Two Fact	J	My Voult (Driveto)	
Stress 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 Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 223 General 224 Information 226 Two Factor 227 Roles 228 Applications 226 Two Factor 227		My Vaul (Privale)	
Session 153 RDP (Microsoft Remote Desktop) 153 Apple Remote Desktop (ARD) 171 Information 176 Alarm Codes 177 Email Account 179 Website 188 Note/Secure Note 188 Contact 189 Document 191 Folder 194 Credential Entry 196 Connection String 197 One-Time Passw ord (OTP) 199 Passw ord (OTP) 199 Passw ord (OTP) 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 215 Diagnostic 219 5 Administration 221 Security Management 222 Users 223 General 224 Information 224 Management 222 Users 223 General 224			
Apple Remote Desktop (ARD) 171 Information 176 Alarm Codes 177 Enail Account 179 Website 188 Contact 189 Document 191 Folder 194 Credential Entry 196 Connection String 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 223 General 224 Information 224 Normation 225 Vers 223 General 224 Administration 225 Qeneral 224 Normation 226 Two Factor 227 Ro		Session	
Apple Vention Desktop (KND) 111 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 Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 215 Scheduling Reports 215 Diagnostic 219 5 Administration 223 General 224 Information 226 Two Factor 227 Roles 228 Applications 228 Vauits 230		RDP (Microsoft Remote Desktop)	
Information 170 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 Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vauits 230		Apple Relible Desklop (ARD)	
Image: Account 179 Email Account 179 Website 186 Note/Secure Note 188 Contact 189 Document 191 Folder 194 Credential Entry 196 Connection String 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 223 Users 223 General 224 Information 225 Tw o Factor 227 Roles 228 Applications 226 Vauits 230		Alarm Codes	
Unlaw Account 100 Website 186 Note/Secure Note. 188 Contact 189 Document. 191 Folder 194 Credential Entry. 196 Connection String. 197 One-Time Passw ord (OTP). 199 Passw ord List 201 Private Key 203 Username/Passw ord. 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 222 Users 223 General 224 Information 225 Vaults 226 Vaults 226		Finail A count	170
Note/Secure Note 188 Contact 189 Document 191 Folder 194 Credential Entry. 196 Connection String. 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 216 Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 225 Valts 226 Vauits 228		Website	186
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 201 Scheduling Reports 211 Configuration 215 Diagnostic 219 5 Administration 223 General 224 Information 226 Two Factor 227 Roles 228 Applications 229 Vaults 230		Note/Secure Note	188
Document. 191 Folder 194 Credential Entry. 196 Connection String. 197 One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Two Factor 223 Querts 223 Quertal 224 Normation 225 Quertal 226 Two Factor 227 Roles 228 Applications 228 Vaults 230		Contact	189
Folder 194 Credential Entry. 196 Connection String. 197 One-Time Passw ord (OTP). 199 Passw ord List 201 Private Key 203 Username/Passw ord. 205 Import 207 4 Reports 211 Configuration 216 Scheduling Reports 215 Diagnostic 219 5 Administration 223 Users 223 General 224 Information 226 Tw o Factor 223 General 224 No Factor 227 Roles 228 Applications 229 Vaults 230		Document	191
Credential Entry. 196 Connection String. 197 One-Time Passw ord (OTP). 199 Passw ord List 201 Private Key 203 Username/Passw ord. 205 Import 207 4 Reports 211 Configuration 216 Scheduling Reports. 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Folder	194
Connection String. 197 One-Time Passw ord (OTP). 199 Passw ord List 201 Private Key 203 Username/Passw ord 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 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Credential Entry	196
One-Time Passw ord (OTP) 199 Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 216 Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Connection String	
Passw ord List 201 Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 214 Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		One-Time Passw ord (OTP)	
Private Key 203 Username/Passw ord 205 Import 207 4 Reports 211 Configuration 215 Scheduling Reports 215 Diagnostic 219 5 Administration 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Passw ord List	
Username/Passw ord 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 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Private Key	
Import 207 4 Reports 211 Configuration 215 Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Username/Passw ord	
4 Reports 211 Configuration 215 Scheduling Reports 215 Diagnostic 219 5 Administration Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Import	
Configuration215Scheduling Reports215Diagnostic2195 Administration221Security Management223Users223General224Information226Tw o Factor227Roles228Applications229Vaults230	4	Reports	
Scheduling Reports 215 Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Configuration	215
Diagnostic 219 5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Scheduling Reports	
5 Administration 221 Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Diagnostic	
Security Management 223 Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230	5	Administration	
Users 223 General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Security Management	222
General 224 Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		lisers	223
Information 226 Tw o Factor 227 Roles 228 Applications 229 Vaults 230		General	224
Tw o Factor 227 Roles 228 Applications 229 Vaults 230		Information	224
Roles 228 Applications 229 Vaults 230		Two Factor	220
Applications 229 Vaults 230		Roles	228
Vaults230		Applications	229
		Vaults	

Email Notifications	
Applications	
Applications	
Vaults	
Users Locked	
Users 2FA Status	
Reset Server Cache	
Notifications	
Subscribers	
Subscriber Groups	
Subscriptions	
Configuration	
System Settings	
General	
System Message	
Passw ord Policy	
Passw ord Template	
Forbidden Passw ord	
Type Availability	
User Template	
Email Notifications	
Advanced	
Passw ord Server Settings	
General	
General	
Authentication	259
Domain	261
Office365	265
Email	268
Logaina	271
Features	273
Scheduler	274
Advanced	275
Security	276
Two-Factor	276
SMS	280
Backun Codes	200
Security	201 295
	203
Brivileged Access Management	207
System Parmingiana	209
System Fermissions	
Hilles	
Management	
Tuuis	
FIVILEGED ACCESS IVIANAGEMENT	
Decouverd Terministee	
Password remplates	
rempiates	
раскир Васкир	
Backup Manager	
Backup List	

Part VI Privileged Access Management

1	Getting Started	. 327
2	Accounts	. 334
3	Providers	. 336
	Domain Provider	. 339
	SQL Server Provider	. 341
4	Scan Configurations	. 345
	Domain Account Discovery SSH Account Discovery SQL Account Discovery	. 349 . 352 . 355
5	Checkout Process	. 358
6	View Sensitive Data vs Account Brokering	. 363

Part VII Devolutions Web Login

300

325

1	Overview	366
2	Installation	367
	Chrome	367
	Firefox	369
	Microsoft Edge Beta	370
	Opera	374
3	First Login	375
	Password Hub	375
	Multiple Passw ord Hub	379
	Password Server	
	Remote Desktop Manager	
4	Exploring Devolutions Web Login	390
	Menu	390
	Settings	390
	Retrieve Credentials	
	Remote Desktop Manager	396
	Secure Devolutions Web Login	397
	Keyboard Shortcuts	399

Part VIII Devolutions Launcher

	-	-
•	n	\mathbf{a}
4	IJ	-5
-	v	~

1	Overview		404
2	Installation		405
	Prerequisito Windows macOS Android iOS	95	405 406 413 414 415
3	Configuration	and Settings	416
	Devolutions	Password Server	416
	Window	S	419
	macOS		423
	Android		428

Devolutions Pass word Hub 436 Android 436 Android 440 4 Utilization 448 Windows and macOs 448 Android and IOS 459 Part IX Support/Resources 453 1< FAQ (Frequently Asked Questions) 454 2< Follow Us 456 3< Previous Versions 457 4 Technical Support 458 5< Knowledge Base 459 Azure portal configuration guide for Offica365 authentication 459 Backup and restore Devolutions Pass word Server 451 Configure Devolutions Pass word Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Devolutions Pass word Server to use integrated security 501 Configure Notifications 506 Configure Notifications 509 Configure Notifications 509 Configure Notifications 509 Configure Notifications 502 Sold Server is answering on a High Availability Topology 514 Manage Encryption Keys on a High Availability Topology 524		iOS	
Windows 436 Android 440 10S 444 4 Utilization 448 Windows and macOs 448 Android and IOS 459 Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 458 6 Knowledge Base 458 7 Configure Cleint Data Source 457 Configure Devolutions Pass word Server 451 Configure Devolutions Pass word Server to us a integrated security 500 How to Grant access to SQL Server instance 601 Configure Venditications 518 Identify which Server is answering on a High Availability Topology 524 Ports And Firewalls 529 Synthch from Shared passphrase to Shared passphrase (v2) 522 SQL Server Express configuration 556 Update your registration serial after a renewal 561 Update your registration serial		Devolutions Password Hub	436
Android		Window s	
LOS 444 4 Utilization 444 Windows and macOs 448 Android and IOS 459 Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 459 5 Knowledge Base 459 Azure portal configuration guide for Office 355 authentication 459 Backup and restore Bvolutions Password Server 459 Configure Orent estore Bvolutions Pass word Server to use integrated security 500 How for ena access to SQL Server to use integrated security 500 How for ena access to SQL Server is tance 501 Configure Ot LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 521 Sot, Server Express configuration 566 Our origit reside accure reside accure is Enply 548 Mater Update your registration serial after a re		Android	
4 Utilization 448 Windows and macOs 448 Android and IOS 450 Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office365 authentication 459 Backup and restore Devolutions Password Server 451 Configure Devolutions Password Server to be always available 457 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 601 Configure Windows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 524 Ports And Firewalls 532 Switch from Shared passphrase to Shared passphrase (v2) 532 Suitch from Shared passphrase to Shared passphrase (v2) 532 Suitch from Shared password Server 2016 544 Updats your registration serial after a renewal		iOS	
Windows and macCe 448 Android and IOS 450 Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Offica358 authentication 459 Backup and restore Devolutions Pass word Server 451 Configure Client Data Source 455 Configure Devolutions Password Server to be always available 456 Configure Outlons Password Server to use integrated security 500 Hw to Grant access to SQL Server instance 501 Configure Whichows Authentication 514 Entrofing usage of LDAPS 514 Identify which Server is answering on a High Availability Topology 524 Ports And Firewalis 529 Sultch from Shared passphrase to Shared passphrase (v2) 522 Sultch from Shared passphrase to Shared passphrase (v2) 522 Sultch from Shared passphrase to Shared passphrase (v2) 522 Sultch from Shared passphrase to Shared passphrase (v2) 522 Sulte Aport<	4	Utilization	448
Android and IOS 450 Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office 365 authentication 459 Azure portal configuration guide for Office 365 authentication 459 Backup and restore Devolutions Password Server 451 Configure Olient Data Source 455 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Nuclifications 509 Configure Windows Authentication 514 Enforcing usage of LDAPS 514 Identify which Server is answering on a High Availability Topology 524 Ports And Firewalls 529 Switch from Shared passphrase to Shared passphrase (v2) 522 SQL Server Express configuration 543 G Troubleshooting 544 Duplicate Devolutions Pass word Server 2016 544 Duplicate Devolutions Password Server 2016 543 <		Windows and macOs	
Part IX Support/Resources 453 1 FAQ (Frequently Asked Questions) 454 2 Follow Us 458 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office365 authentication 459 Azure portal configuration guide for Office365 authentication 459 Configure Devolutions Pass word Server 451 Configure Devolutions Pass word Server to use integrated security 500 How to Grant access to SOL Server instance 501 Configure Bustons 516 Configure StL 509 Configure StL 509 Configure Windows Authentication 516 Configure StL 509 Streer Express configuration 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a Hig		Android and iOS	450
1 FAQ (Frequently Asked Questions) 454 2 Follow Us 456 3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office 365 authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 497 Configure Clent Data Source 495 Configure Devolutions Pass word Server to be always available 497 Configure Devolutions Pass word Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Windrows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 522 Sult Server Express configuration 543 Update your registration serial after a renewal 540 Update your registration serial after a renewal 543 Blank login page on a Windows Server 2016 544 Parts Agent 543 Blank login page on a Wind	Part IX	Support/Resources	453
2 Follow Us	1	FAQ (Frequently Asked Questions)	454
3 Previous Versions 457 4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office365 authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 487 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to be always available 501 Configure Devolutions Password Server to be always available 501 Configure Devolutions Password Server to be always available 501 Configure Devolutions Password Server to be always available 501 Configure Bothins Password Server to be always available 501 Configure SL 500 Configure SUL 502 Configure Windows Authentication 514 Identify which Server is answering on a High Availability Topology 524 Ports And Firewalls 529 Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 543 Update your registration serial after a renewal <td< td=""><td>2</td><td>Follow Us-</td><td> 456</td></td<>	2	Follow Us-	456
4 Technical Support 458 5 Knowledge Base 459 Azure portal configuration guide for Office 365 authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 487 Configure Client Data Source 487 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance. 501 Configure Windows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 522 SQL Server Express configuration 543 Update your registration serial after a renewal 543 Ubdate your registration serial after a renewal 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544	3	Previous Versions-	457
5 Knowledge Base 459 Azure portal configuration guide for Office 365 authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 487 Configure Client Data Source 495 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure Windows Authentication 614 Enforcing usage of LDAPS 618 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 522 SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Failed Request Tracing in IIS 556 Enable Failed Requ	4	Technical Support	458
Azure portal configuration guide for Office365 authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 487 Configure Cilent Data Source 495 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure SSL 509 Configure SU 509 Configure SSL 509 Switch from Shared passphrase to Shared passphrase (v2) 522 SQL Server Express configuration 536 Update your registration serial after a renewal 543 G Trouble shooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 B	5	Knowledge Base	459
Azure portal computation guide for Orice ass authentication 459 Backup and restore Devolutions Password Server 481 Command Line Interface 487 Configure Client Data Source 495 Configure Devolutions Pass word Server to be always available 497 Configure Devolutions Pass word Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure SUL 609 Configure Windows Authentication 614 Enforcing usage of LDAPS 618 Identify which Server is answering on a High Availability Topology 524 Ports And Firew alls 529 Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 543 Update your registration serial after a renewal 543 Outser Agent 543 After Upgrading Server the Devolutions Pass word Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Pass word Server is Empty 543 Blank login page on a Windows Server 2016 544 Failed Request Tracing in IIIS	5	Anno portal configuration muide for Office 205 outbourtier	
Command Line Interface 481 Configure Client Data Source 495 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Nutifications 506 Configure Windows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 522 Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 543 G Toroble shooting 543 A After Upgrading Server the Devolutions Password Server is Empty 543 G Touble shooting 554 Error Uploading Document 554 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing Ing IIS 557 Configure Failed Request Tracing IIS 557 Configure Failed Request Tracing IIS 557 Configure Failed Request Tracing IIS 572 T		Azure portal configuration guide for Office365 authentication	
Configure Client Data Source 495 Configure Devolutions Password Server to be always available 497 Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure Notifications 509 Configure Notifications 501 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 522 SQL Server Express configuration 532 SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 G Troubleshooting 544 After Upgrading Server the Devolutions Password Server is Empty 543		Command Line Interface	
Configure Devolutions Password Server to be always available497Configure Devolutions Password Server to use integrated security500How to Grant access to SQL Server instance.501Configure Notifications506Configure SSL509Configure Windows Authentication514Enforcing usage of LDAPS518Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology522SQL Server Express configuration536Update your registration serial after a renewal540User Agent543After Upgrading Server the Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document556Enable Failed Request Tracing in IIS557Configure Express renew al means563Could Request Tracing in IIS557Configure Bailed Request Tracing in IIS557Configure Bailed Request Tracing in IIS557Configure Failed Request Tracing in IIS557Configure Failed Request Tracing in IIS557The remote server returned an error: (400) Bad Request572The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Configure Client Data Source	
Configure Devolutions Password Server to use integrated security 500 How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure SL 509 Configure Windows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 524 Ports And Fire walls 529 SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 G Trouble shooting After Upgrading Server the Devolutions Pass word Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Pass word Server instance 546 Error Uploading Document 554 Failed Request Tracing in IIS 556 Configure Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 577 The remote server returned an error (405) Method Not Allowed 577 The encryption file i		Configure Devolutions Password Server to be always available	
How to Grant access to SQL Server instance 501 Configure Notifications 506 Configure Windows Authentication 514 Enforcing usage of LDAPS 518 Identify which Server is answering on a High Availability Topology 521 Manage Encryption Keys on a High Availability Topology 524 Ports And Firewalls 529 Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 536 Update your registration serial after a renewal 543 User Agent 543 After Upgrading Server the Devolutions Pass word Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Pass word Server instance 546 Error Uploading Document 556 Enable Failed Request Tracing with IIS 556 Configure Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error: (405) Method Not Allowed 577 The encryption file is missing 580		Configure Devolutions Password Server to use integrated security	497 500
Configure Notifications506Configure SSL509Configure Windows Authentication514Enforcing usage of LDAPS518Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology524Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent543 6 Troubleshooting544Duplicate Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server is Empty543Failed Request Tracing with IIS556Enable Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request570The encryption file is missing580		How to Grant access to SQL Server instance	501
Configure SSL509Configure Windows Authentication514Enforcing usage of LDAPS518Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology524Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent5436Troubleshooting544Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server is Empty543Failed Request Tracing with IIS556Enable Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Configure Notifications	506
Configure Windows Authentication514Enforcing usage of LDAPS518Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology524Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent5436Trouble shooting544Duplicate Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document556Failed Request Tracing with IIS556Enable Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Configure SSL	
Enforcing usage of LDAPS518Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology524Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent5436Troubleshooting543After Upgrading Server the Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document556Failed Request Tracing with IIS556Enable Failed Request Tracing in IIS557Configure Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Configure Windows Authentication	
Identify which Server is answering on a High Availability Topology521Manage Encryption Keys on a High Availability Topology524Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent5436 Troubleshooting543After Upgrading Server the Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document554Failed Request Tracing with IIS556Enable Failed Request Tracing In IIS557Configure Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Enforcing usage of LDAPS	
Manage Encryption Keys on a High Availability Topology 524 Ports And Firewalls 529 Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 6 Troubleshooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Pass word Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Identify which Server is answering on a High Availability Topology	
Ports And Firewalls529Switch from Shared passphrase to Shared passphrase (v2)532SQL Server Express configuration536Update your registration serial after a renewal540User Agent5436 Trouble shooting543After Upgrading Server the Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document554Failed Request Tracing with IIS556Enable Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Manage Encryption Keys on a High Availability Topology	524
Switch from Shared passphrase to Shared passphrase (v2) 532 SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 6 Troubleshooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Ports And Firewalls	529
SQL Server Express configuration 536 Update your registration serial after a renewal 540 User Agent 543 6 Trouble shooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Consult the Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Switch from Shared passphrase to Shared passphrase (v2)	532
Update your registration serial after a renewal 540 User Agent 543 6 Troubleshooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing log. 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		SQL Server Express configuration	536
User Agent 543 6 Troubleshooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Update your registration serial after a renewal	540
6 Trouble shooting 543 After Upgrading Server the Devolutions Password Server is Empty 543 Blank login page on a Windows Server 2016 544 Duplicate Devolutions Password Server instance 546 Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing 563 Consult the Failed Request Tracing log. 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allow ed 577 The encryption file is missing 580		User Agent	543
After Upgrading Server the Devolutions Password Server is Empty543Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document554Failed Request Tracing with IIS556Enable Failed Request Tracing in IIS557Configure Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580	6	Troubleshooting	543
Blank login page on a Windows Server 2016544Duplicate Devolutions Password Server instance546Error Uploading Document554Failed Request Tracing with IIS556Enable Failed Request Tracing in IIS557Configure Failed Request Tracing563Consult the Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		After Upgrading Server the Devolutions Password Server is Empty	543
Duplicate Devolutions Password Server instance546Error Uploading Document554Failed Request Tracing with IIS556Enable Failed Request Tracing in IIS557Configure Failed Request Tracing563Consult the Failed Request Tracing log571IIS Logging572The remote server returned an error: (400) Bad Request576The remote server returned an error (405) Method Not Allowed577The encryption file is missing580		Blank login page on a Windows Server 2016	544
Error Uploading Document 554 Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing 563 Consult the Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Duplicate Devolutions Password Server instance	546
Failed Request Tracing with IIS 556 Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing 563 Consult the Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Error Uploading Document	554
Enable Failed Request Tracing in IIS 557 Configure Failed Request Tracing 563 Consult the Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Failed Request Tracing with IIS	556
Configure Failed Request Tracing 563 Consult the Failed Request Tracing log 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Enable Failed Request Tracing in IIS	557
Consult the Failed Request Tracing log. 571 IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Configure Failed Request Tracing	563
IIS Logging 572 The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		Consult the Failed Request Tracing log	
The remote server returned an error: (400) Bad Request 576 The remote server returned an error (405) Method Not Allowed 577 The encryption file is missing 580		IIS Logging	572
The remote server returned an error (405) Method Not Allowed577 The encryption file is missing580		The remote server returned an error: (400) Bad Request	576
The encryption file is missing		The remote server returned an error (405) Method Not Allowed	577
		The encryption file is missing	

Overview

Part I

1 Overview

1.1 What is Devolutions Password Server?

DESCRIPTION

This documentation is valid for version 2020.1.0. Previous Versions



Devolutions Password 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 Password Server:



Web browser access and Devolutions Web Login	Using a client application (desktop or mobile)
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. With the Devolutions Web Login browser extension, credentials can be automatically submitted when connecting to a website.	Access vaulted resources using our client applications which communicate with Devolutions Password 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.
Remote access technologies (RDP, VNC, etc) are not supported within a web browser.	Unlike with web browser access, Remote Desktop Manager can launch sessions using remote access technologies.

HIGHLIGHTS



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 exposed publicly on the Internet or only to your Intranet or private cloud.
TWO-FACTOR AUTHENTICATION	EMAIL NOTIFICATIONS	IP RESTRICTIONS
Widest choice of <u>Two-</u> <u>factor authentication</u> (2FA) providers. Many providers can be enabled concurrently. They can selectively be enforced per user.	Optionally receive email notifications for various events on sessions, users, roles, etc.	Controlling access to Devolutions Password Server from IP addresses / ranges, including GeoIP restriction and IP whitelisting / blacklisting.

1.2 System Requirements

MINIMUM REQUIREMENTS



Devolutions Password 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).
- 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 <u>requirements for the .Net</u> <u>Framework</u> 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 Password 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 <u>Topology</u>.

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 Password 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 then the latter.

64-BIT SUPPORT

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

1.3 **Topologies**

DESCRIPTION

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

SINGLE SERVER TOPOLOGY

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



Single Server Installation

RECOMMENDED BASIC TOPOLOGY

A recommended basic topology consists of two servers, one for the Devolutions Password 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.



Basic Topology

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 Password Server is still accessing the data source and is transparent for Remote Desktop Manager users.



High Availability Topology

LOAD BALANCING TOPOLOGY

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



Load Balancing Devolutions Password Server Topology

DEVOLUTIONS PASSWORD 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 Password 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 Password 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:

- <u>Synchronizers</u>, particularly the one for RDM data.
- PowerShell scripting (to export a specific branch of your tree).

Getting Started

Part II

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 <u>Getting Started - Team Edition</u>.

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 Password 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 Password Server can be installed through different topologies.

DOMAIN REQUIREMENTS

These requirements apply especially if you intend to use Automatic User Account Creation (see <u>Authentication</u>) and/or <u>Roles</u> 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 PASSWORD SERVER

SOFTWARE REQUIREMENTS ON THE SERVER HOSTING THE INSTANCE

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

INSTALLATION STEPS



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 Password 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 Password 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 <u>Encrypting</u> <u>Connections to SQL Server</u>.

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

2.1.2 Encrypting Connections to SQL Server

DESCRIPTION

To ensure that the communication between the Devolutions Password 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 <u>Encrypting</u> <u>Connections to SQL Server (technet)</u>.

After proper configuration, the only modification required in Devolutions Password Server is to enable the **Use SQL Server encrypted connection** in the <u>Database</u> 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 Password Server.

The installation procedure is available at **Devolutions Password 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 <u>Authentication</u>) and/or <u>Roles</u> 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



INSTALLATION STEPS

~	Create a new instance of Devolutions Password Server (see <u>Create</u> <u>Devolutions Password Server Instance</u>).
~	Create a Devolutions Password Server administrator account in the <u>User</u> <u>Management</u> .
~	Create Roles (see <u>Role Management</u>).
~	Add domain users or built-in users (see <u>User Management</u>).

Installation

Part III

3 Installation

TOPOLOGY

If you just have received your license serials, please refer to the <u>Getting</u> <u>Started</u> topic.

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

The recommended <u>topology</u> 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 <u>Download page</u>.



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



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 <u>http://support.microsoft.com/kb/316898</u>. 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 PASSWORD 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 <u>http://localhost</u>. **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 PASSWORD SERVER INSTANCE

Please refer to the Create Devolutions Password Server instance topic.

3.1 Installing Web Roles Prerequisites

DESCRIPTION

The installation of the Devolutions Password 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 Password Server.

As a web application, Devolutions Password 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 Password Server



Installing prerequisites from <u>Devolutions Password Server Console</u> or from the PowerShell script require internet access to download <u>Web</u> <u>Platform Installer</u> and <u>URL Rewrite Module</u>.

STEPS

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

1. Devolutions Password Server Console

- a. Open the <u>Devolutions Password Server Console</u>.
- **b.** Expand the <u>Advanced</u> menu and select <u>Check Prerequisites</u>.
- c. Click on the Install Prerequisites button to run the PowerShell script.

Devolutions Password Server Console - IIS Features Diagnostic	
IIS Features Diagnostic	
Feature	
Static Content	~
Default Document	 Image: A second s
Directory Browsing	1
HTTP Errors	1
Application Initialization	✓
ISAPI Extensions	✓
ISAPI Filters	~
ASP.NET 4.5	✓
HTTP Logging	~
Basic Authentication	1
Windows Authentication	~
Static Content Compression	~
IIS Rewrite Module	
C Install Prerequisites	Close

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)



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.



PowerShell Window

2. 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.



IIS Installation

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



Web Roles Installation

3.2 Database Instance

DESCRIPTION

Devolutions Password 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 Password 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 <u>Configure Devolutions Password Server to use integrated security</u> for instructions that need to be performed <u>after</u> creating the Devolutions Password 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**. <u>Download SQL</u> <u>Server 2017 Express from Microsoft's site</u>.

If full integration with Active Directory is required, you can decide to activate Windows Authentication solely. Please refer to the <u>MSDN online help</u> 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 Pa	word Server Console - Password Server Settings – 🛛	×
Passw	rd Server Settings	
General	Database	
Database		
Authentication	Host	-
Domain	Database	
Office365	Using Management Tools Credentials	
IIS	Advanced Settings	- I
Advanced	Credentials Test Server	
	Create Database	
	Test Database	
	Management Tools	1
	Username	
	Email Schema to Support	
	View Database Version	
	Scheduler Service	_
	Username Test Scheduler Credentials	
	Password	
	Web Application	
	Username Test Web Application Credentials	
	Passworu	
	Search property	ncel

Devolutions Password Server Console - Database Tab

3.3 Create Devolutions Password Server instance

DESCRIPTION

If you have recently received your serial licenses keys, please refer to the <u>Getting Started</u> topic.



For more information about any of the features in the deploy wizard, please consult their respective topic under the <u>Server Settings</u> chapter.

Multiple Devolutions Password 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 <u>Download</u> 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.
| 👔 Devo | utions Password Server Console | | | × |
|-----------|--|-----------------|--|---|
| C 🕯 i | a d 🕼 👘 🖉 🖉 📾 🖉 🖬 🔛 🗛 | | | : |
| Actions | Details | | | |
| | Name | Version | | |
| Edit | Description | | | |
| | Serial (server) | | | |
| + | | | | |
| New | | | | |
| × | Deploy a new Devolutions Password Server | Web application | | |
| Delete | Default path | | | |
| Deleter | Application pool | Runtime version | | |
| 3 | Authentication | | | |
| R.C | Scheduler service | | | |
| Upgrade S | rver | Go Offline | | |
| | | | | |
| | | | | |
| | | | | |

Deploy a new Devolutions Password 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 Password Server. Missing features are marked with an �. The Install Prerequisites button will install all missing features using a PowerShell script.

Devolutions Password Server Console - Checking IIS Prerequisites for Installation				
Checking IIS Prerequisites for Installation				
Feature				
HTTP Errors	~			
HTTP Logging	~			
Static Content	~			
Default Document	~			
Directory Browsing	~			
Application Initialization	~			
ASP.NET 4.7	~			
ISAPI Extensions	~			
ISAPI Filters	~			
Basic Authentication	~			
Static Content Compression	~			
Windows Authentication	•			
IIS Rewrite Module	~			
Continue Continue	ancel			

IIS Features Diagnostic Dialog

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

Devolutions Password Server Console - Devolutions Password Server Dep	ploy Wizard		-		×		
Devolutions Password Server Deploy V	Vizard						
End User License Agreement							
LICENSE AGREEME	NT				^		
Devolutions [®] Password Server							
This License Agreement applies to the Devolutions® Password Server software.							
IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWIN START USING THE SOFTWARE. THIS AGREEMENT CONTAINS A MANDATORY ARE	ING LEGAL AGI BITRATION CLA	REEMENT BEFC <u>USE.</u>	DRE YOU DOW	VNLOAD	OR		
BY INSTALLING OR USING THE SOFTWARE FOR THE PURPOSES PERMITTED HEREIN, YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. SUCH ACTION IS A CONFIRMATION OF YOUR CONSENT TO BE BOUND BY, AND TO BECOME A PARTY TO, THIS AGREEMENT. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN AGREEMENT SIGNED BY YOU; IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU SHALL REFRAIN FROM INSTALLING OR USING THE SOFTWARE. YOU CONFIRM AND ACKNOWLEDGE THAT YOU HAVE BEEN PROVIDED THE OPPORTUNITY TO READ THE AGREEMENT BEFORE INSTALLING OR USING THE SOFTWARE. A COPY OF THIS AGREEMENT IS MADE AVAILABLE AND MAY BE DOWNLOADED FROM DEVOLUTIONS' WEBSITE.							
This Agreement is entered into between You and Devolutions and establishes the terms and conditions under which we agree to grant You and the Users 🗸							
\checkmark I agree to the terms in the License Agreement							
	Previous	Next	Install	Can	icel		

Devolutions Password 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 <u>Database</u> 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. Please consult <u>How to Configure Devolutions</u> <u>Password Server to use integrated security</u>.

Devolutions	s Password Server Console - Dev	olutions	Password Server Deploy Wizard		-		×
Dev	volutions Password	l Serv	er Deploy Wizard				
Database							
Host	LOCALHOST\SQL2017		Microsoft SQL Server 👻				
Database	DPS		Using Management Tools Credentials				
	Advanced Settings		Test Server				
Credentials	ees with		Create Database				
Integrated	security		Test Database				
Management T	iools		Update Database				
Username	VaultOwner		Email Schema to Support				
Password	•••••		View Database Version				
Scheduler Serv	rice						
Username	VaultScheduler		Test Scheduler Credentials				
Password	•••••						
Web Applicatio	n						
Username	VaultRunner		Test Web Application Credentials				
Password	•••••						
			Previous Next	Ins	tall	Cano	cel

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 <u>Database</u> topic for further information.

Devolutions Password Server Console - Create database		×
😂 Create database		
 Create vault with restricted access by default Allow templates (local) Allow local password templates Allow sub connections 		
Use legacy security ✓ Enable pwned check by default		
ОК	Can	cel

Create daTabase Dialog

Devolutions Password Server Console	×
Database creation successful!	
	ОК

Database Creation Successful Dialog

 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 Password Server license yet, you may <u>Request a</u> <u>30-days trial</u>.

Devolutions Pass	word Server Console - Devolutions Password Server Deploy Wizard – 🗆 🗙
Devolu	itions Password Server Deploy Wizard
General	
Name	Devolutions Password Server
Description	
Serial	
Server	Request Trial
User CAL	10
Launcher CAL	10
Information	
Edition	Platinum
Expiration	Saturday, October 15, 2033
	Previous Next Install Cancel

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 Password Server instance within this folder.

We do not recommend to set the installation folder to *C:\Program Files* or *C:\Program Files (x86)*. Devolutions Password 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.

Devolutions Password Server Console - Devolutions Password Server De	ploy Wizard		-		×
Devolutions Password Server Deploy	Wizard				
Installation Source					
Download from the web (latest version)					
○ Install from zip file					
Installation Destination					
Web application name					
dps					
Installation folder					
C:\inetpub\wwwroot\dps					
	Previous	Next	Install	Cancel	I

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 Password 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 <u>Authentication</u> <u>server settings</u> topic for further information.

Devolutions Password Server Console - Devolutions Password Server Deploy Wizard	-		×
Devolutions Password Server Deploy Wizard			
Authentication Modes			
Authenticate with domain user			
Authentication with database [Deprecated]			
Authenticate with Office365 user			
Authenticate with local machine user [Deprecated]			
✓ Authenticate with Devolutions Password Server custom user			
Windows Authentication			
Enable Windows authentication			
3 Windows authentication requires further configuration on your IIS server. Please dick the Help button for instructions.		8	
Previous Next In	istall	Cance	el

Authentication Modes Dialog

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

Devolutions Password Server Console - Devolutions Password Server Deploy Wizard								×		
Devolution	is Password	Serve	er De	ploy W	/izard					
IIS Settings										
Website	Default Web Site	-	Ŧ	Diagnostic	S					
Force https This option require documentation on	s that you install an SS the steps to follow.	L certificate	in IIS. Ple	ase see IIS						
Encrypt web.config file										
Web application name										
dps										
					Previous	Next	I	install	Cano	el

IIS Settings Dialog

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

Devolutions Password Se	Devolutions Password Server Console - Devolutions Password Server Deploy Wizard –			
Devolution	s Password Server Deploy Wizard			
DPS console password setup -			-]	
Disable DPS console passwo	ord validation			
Password	Ø			
Confirm Password	•			
	Previous Next Install	Cancel		

Devolutions Password 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 : <u>Backup</u> <u>manager</u>, <u>Domain Users and Roles cache</u>, <u>Office365 Users and Roles cache</u>, Email notifications and <u>Privileged Access Management</u>.

Devolutions Password Ser			×			
Devolutions	Password Server Deploy	Wizard				
Scheduler						
✓ Install Scheduler service						
Service Account						
Predefined account	LocalService -					
○ This account						
Password						
Confirm Password						
		Previous	Next	Install	Cano	el

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.

Devolutions Password Server Console - Devolutions Password Server Deploy Wiz	zard				×
Devolutions Password Server Deploy Wizar	rd				
Settings					
General Name: Devolutions Password Server Description: Serial: XXXXX-XXXXX-XXXXX-XXXXX- Database Server: LOCALHOST\SQL2017 Database: DPS IIS Settings Website: Default Web Site .NET Framework version: v4.0 Installation Destination Web application name: dps Installation folder: C:\jinetpub\www.root\dps					•
4				Þ	
Prev	/ious	Next	Install	Canc	el

Settings Dialog

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



Devolutions Password Server Console - Backup Encryption Keys				
🚹 Backuj	p Encryption Keys			
Web Application IMPORTANT: Kee	ep this file in a secure backup location			
Password	••••••			
Filename	C:\Temp\EncryptionKeys.bin	Select File		
		OK		

Backup Encryption Keys Dialog

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

Devolutions Password Server Console - Devolutions Password Server Deploy	y Wizard				×
Devolutions Password Server Deploy Wiz	zard				
Progress Upgrading database for data source 'DPS' with version 573 EXECUTED Up to black of the temperature of					•
Upgrading database for data source 'DPS' with version 574 Upgrading database for data source 'DPS' with version 574 EXECUTED					
Upgrading database for data source 'DPS' with version 575 Upgrading database for data source 'DPS' with version 575 EXECUTED					
Upgrading database for data source 'DPS' with version 576 Upgrading database for data source 'DPS' with version 576 EXECUTED					
Upgrading database for data source 'DPS' with version 577 Upgrading database for data source 'DPS' with version 577 EXECUTED					
Upgrading database for data source 'DPS' with version 578 Upgrading database for data source 'DPS' with version 578 EXECUTED					
Upgrade database Done! Generating encryption fileDone! Saving DPS Console password configurationDone! Configuring the web.configDone! Install and start scheduler serviceDone! Deployment completed!					
4				Þ	•
	Previous	Next	Install	Clos	e

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 Password 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 Password Server authentication, create an administrator account and grant the Administration privilege to the account. Please refer to <u>User Management</u> for further information about creating user accounts.

After the successful authentication with the other model, the Devolutions Password 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 Password Server authentication model. Please see Automatic User Account Creation section in the topic <u>Authentication</u>.

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** ^(S) button in the Devolutions Password Server Console.

Devolutions	Password Server Console		_		×
C i 🖬 🖻	🍓 📚 📦 👼 🗛 🗮	<mark>9</mark> 🗖 🏭 🔒			:
Actions	Details	Browse the Devolutions Password Server Web Site			
	Name	Devolutions Password Server Version	2019.2.	12.0	
Edit	Description				
	Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-ENVTY Platinum			
+		Saturday, October 15, 2033			
New	Serial (user CAL)	XXXXX-XXXXX-XXXXX-24FLN 10			
	Launcher CAL serial	XXXXX-XXXXX-XXXXX-XXXXX-GZNN5 10			
X	Website	Default Web Site Web application	/dps		
Delete	Default path	C:\inetpub\www.root\dps			
Delete	Application pool	dps Runtime version	v4.0		
	Authentication	DVLS Custom			
K Ø	Scheduler service	Running			
Upgrade Server		Go Offline			
o ^o		<u>Kanana kanana kanan</u>	3		
Uninstall Scheduler					
2019.2.12.0					

Devolutions Password Server Console

To test the connection from a client by creating a data source in Remote Desktop Manager. Please consult the <u>How to Configure Client Data Source</u> for more information.

3.4 Upgrading Devolutions Password Server

UPGRADE

Install the proper version of Devolutions Password Server Console before upgrading the Devolutions Password Server web application. It is available on the <u>Download page</u>.

1

Since Devolutions Password Server 2019.x, many features can only be managed from the web interface. Please see <u>Administration -</u> <u>Password Server Settings</u>.

It is highly recommended as a best practice to first deploy the new version of Devolutions Password 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 Password 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 Password Server that you are preparing to install. Please follow the steps carefully.

0

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.

Ð

If you have set the <u>Security Provider</u> Passphrase v1 on your current Devolutions Password Server, specific operations will need to be done before the upgrade. Please contact us for further details. We recommend doing a backup of the <u>Encryption Keys</u> 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 Password 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 Password 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 <u>Devolutions Password Server Console</u>.
- 2. Select the instance that you wish to upgrade.

- 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 Pa	assword Server Console			_		\times
	👃 🎝 Import Users 🌷 🍞 👼	D 🖬	S 🖬 🛢 🔚			:
Actions	Details					
	Name		Devolutions Password Server	Version	6.1.3.0	
Edit	Description					
	Serial (server)		XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-ENVTY	Platinum		
-				Saturday, October 15, 2033		
New						
X	Website		Default Web Site	Web application	/dps	
Delete	Default path		C:\inetpub\wwwroot\dps			
	Application pool		dps	Runtime version	v4.0	
	Authentication		Domain, DVLS Custom			
Upgrade Server	Scheduler service		Stopped			
				Go Offline		
	de server					
Uninstall						
Scheduler						
2019.1.9.0						

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 Password Server Console - Devolutions Password Server Upgrade Wizard -		×
Devolutions Password Server Upgrade Wizard		
Upgrade Source		
··· Previous Next Upgrade	C	ancel

Devolutions Password Server Upgrade Wizard

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

Devolutions Password Server Co	nsole - Devolutions Password Se	rver Upgrade Wizard	_		\times
Devolutions Pass	word Server Upgrad	e Wizard			
Settings					
Stopping the web applicationDone! Stopping scheduler serviceDone! Backing up the configurationDone! Backing up filesDone! Unzipping contentDone! Installing contentDone! Upgrading databaseDone! Upgrading databaseDone! Updating encryption fileDone! Updating encryption fileDone! Restoring the configuration Checking .NET Framework runtime Saving connection string in web.config Saving connection string in web.config Saving encryption configuration Done! Restoring the custom foldersDone! Install scheduler serviceDone! Install scheduler serviceDone! Starting scheduler serviceDone! Starting the web applicationDone! Upgrade to version 2019.1.9.0 completed!					< >
	Previous Next		Upgrade	Clo	ose

Upgrade completed

 Since Devolutions Password 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 Password Server Upgrade Wizard dialog.

Devolutions Password Server C	Console - Devolutio	ns Password Se	rver Upgrade V	Vizard —		×
Devolutions Pas	sword Serv	er Upgrad	e Wizard			
Settings						
Stopping the web applicationDone! Stopping scheduler serviceDone! Backing up the configurationDone! Backing up filesDone! Unzipping contentDone! Installing contentDone! Upgrading databaseDone! Restoring encryption fileDone! Updating encryption fileDone! Updating encryption fileDone! NET Framework runtime Saving settings in database Saving settings in database Saving settings in database Saving settings in database Saving connection string in web.config Saving mails configuration in web.config Saving the custom foldersDone! Install scheduler serviceDone! Starting scheduler serviceDone! Starting the web applicationDone! Upgrade to version 2019.1.9.0 completed	ig !					*
<	_	1			[*******	>
Open Backup Folder	Previous	Next		Upgrade	Clo	ose
Open Installation Folder View Installation Log						

FINAL PHASE



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 <u>Database</u> 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 Password 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 IV

4 Management

4.1 Devolutions Password Server Console

DESCRIPTION

Because Devolutions Password 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 <u>Download page</u>.



Since Devolutions Password Server 2019.x, many features can only be managed from the web interface. Please see <u>Administration</u> - 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 P	assword Server Console			-	- 🗆	\times
	🛔 🎝 Import Users 🏽 🍘 🖗) 🗟 🕲 🖬 🛢 🔚				:
Actions	Details		_	Check Prerec	uisites	
	Nama	Develutions Decemend Server	. 🕀	Database Dia	gnostic	
	Name	Devolutions Password Server	•	Send Diagno	stic to Supp	port
Edit	Description			View Installat	tion Logs	
	Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-	E	Open Backup	Folder	
			s 👝	Manage Eng	votion Key	
			**	interlage Erret	yption key	
New			1	Check for Up	dates	
	Launcher CAL serial	XXXXX-XXXXX-XXXXX-XXXXX-K4DRA	1 🕣	About		
X	Website	Default Web Site	Weba	application	/dps	5
Delata	Default path	C:\inetpub\wwwroot\dps				
:	Application pool	dps	Runti	Runtime version v4.0		D
	Authentication	Domain, DVLS Custom				
K Ø	Scheduler service	Running				
Upgrade Server				C- 049:		
				Go Omine		
o°						
Uninstall Scheduler						
2019.1.8.0						

Devolutions Password Server Console

SETTINGS

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

4.1.1 Devolutions Password Server Settings

4.1.1.1 General

DESCRIPTION

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

Devolutions Password Server Console - Password Server Settings					×	
Password	d Server Settin	igs				
General	General					
Database						
Authentication	Name	Devolutions Password Server				
Office365	Description					
IIS		Enable new version mode				
Advanced	Coriol					
	Sena					
	Server	•••••••••••••••••••••••••••••••••••••••	Request T	<u>rial</u>		
	User CAL	••••••	10			
	Launcher CAL	•••••••	10			
	Information					
	Edition	Platinum				
	Expiration	Saturday, October 15, 2033				
	Search property	A	[Save	Cano	el

General Tab

SETTINGS

GENERAL

Name	Enter the name for your server, it will be displayed in the Content area.

Description	Enter a short description or additional information.

SERIAL

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

INFORMATION

Edition	Display the Devolutions Password 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 Password Server.

Devolutions Para	ssword Server Conso	ole - Password Server Setting	IS	-	-		×	
Passw	ord Server S	ettings						
General	Database							
Database								
Authentication	Host	VWINDSRV-SQL\SQL2016		SQL Server		~		
Domain	Database	DBS		SQL Server				
Office365	Database	DF3		SQL Azure	- Kala			
IS		Advanced Settings		Using Management Tools Creden	ittais —			
Advanced				Test Server				
	Credentials	Credentials			Create Database			
	Integrated s	ecurity						
				Test Database				
	Management To	Management Tools Username VaultOwner		Update Database				
	Username					_		
Password			Email Schema to Support		oort			
	1 doshord			View Database Version				
	Scheduler Service							
	Username	VaultScheduler		Test Scheduler Creder	ntials			
	Password	•••••		L				
	Web Application	۱						
	Username	VaultRunner		Test Web Application Cre	edentials			
	Password							
	1 455/1014							
	Search property	2 1		Save	2	Cano	cel	

Database Tab

SETTINGS

DATABASE

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.

Advanced Settings	Access the <u>Advanced Settings</u> .
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 Password Server communicates with the SQL database. These options do not have any impact on how users will authenticate on the Devolutions Password Server instance.

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

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 Serve	r Console - SQL Server	—		\times
SQL Server				
Failover partner Connection minimun pool size Connection maximum pool size Connection retry count Connection retry interval Connection timeout	Use SQL Server encrypted connect Trust server certificate	ion]		
		OK	Ca	ncel

Advanced Settings Dialog

SETTINGS

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.
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 Password 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.

Devolutions Passwor	d Server Console - Password Server Settings	-		×
Password	d Server Settings			
General Database Authentication Domain Office365 IIS Advanced	Authentication Modes ✓ Authenticate with domain user Authentication with database [Deprecated] ✓ Authenticate with Office365 user Authenticate with local machine user [Deprecated] ✓ Authenticate with local machine user [Deprecated] ✓ Authenticate with Devolutions Password Server custom user Windows Authentication ✓ Enable Windows authentication ✓ Windows authentication requires further configuration on your IIS server. Please did Windows authentications.	dk the	0	
	Search property	Save	Cance	el

Authentication Tab

SETTINGS

AUTHENTICATION MODES

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.

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

WINDOWS AUTHENTICATION

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

4.1.1.3.1 Domain

DESCRIPTION

The domain is used to authenticate the user. <u>This is the most secure, flexible and</u> <u>easiest to manage</u>. No need to sync users between the domain and Devolutions Password Server. On first use of the Devolutions Password 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 Password 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.

Devolutions Passwo	ord Server Console - Password Serve	er Settings	_		×
Passwor	d Server Settings				
General	Domain Authentication				
Database					
Authentication	Domain	windjammer.loc			
Domain	Administration credentials	david@windiammer.loc			
Office365	Administration a caenadis	advid@wildjammer.ioc	· · · · ·		
IIS Advanced		Allow logins using email address			
Auvanceu	LDAPS				
		Deut.			
	Enable LDAPS	Port			
		Default			
		O Custom			
	Automatic User Creation				
	Auto create domain users in database				
		Create read-only user			
	Default Vault	Default	~		
	Only from this AD group	RDM Users	×		
		Username Format			
		UPN O Netbios	O Username		
	Multi Domain				
	✓ Multi domain				
	Trusted domains	nino.windjammer.loc	X		
	Domain Users And Roles Cache				
	Enable domain cache feature				
	Update users and groups data every:	0 A Hours 30	minutes		
	Search property		Save	Cance	9

Domain Tab

SETTINGS

DOMAIN AUTHENTICATION

Domain	Specify the remote computer domain name.

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 Password Server instance. The email address field must be filled in the User Management.

LDAPS

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

AUTOMATIC USER CREATION

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.
Username Format	 Select the username format that will be created in the database. 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



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

DOMAIN USERS AND ROLES CACHE

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 Password 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 <u>Azure portal configuration guide for Office 365 authentication</u>.

HOW TO CONFIGURE OFFICE 365 AUTHENTICATION

Overview about Office365 configuration: see <u>knowledge base article</u> for more information

The Office365 tab allows Devolutions Password Server to authenticate users using Office365 authentication. All fields are mandatory.
Devolutions Pas	sword Server Console - Passwo	ord Server Settings		_		×
Passw	ord Server Settings					
General	Office 365 Parameters					
Database					_	
Authentication	Tenant ID	4	a			
Office365	Native application (RDM)					
IIS	Client ID	a	2			
Advanced	Resource ID	0	0		=	
			0		-	
	Redirect URI	http://				
	Web application					
	Client ID	d	9			
	Users and Roles Cache					
	Client ID	3	5			
	Redirect URI	http://				
	Secret key	•••••				
	Automatic User Creation	ers				
	Default Vault	Default	~			
	Office 365 Users And Roles Cach	ne				
	Update users and groups dat	a every: 0 ^ Hours 30	minutes			
	Test Connection					
	Search property	A		Save	Can	icel

Office365 Tab

SETTINGS

OFFICE365 PARAMETERS

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

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

Users and Roles Cache	
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

Auto create Office365	Automatically create the Office365 user account in the

users	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

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 Password Server, the IIS Settings tab is used more as an informative source rather than configuration.

Devolutions Password Server Console - Password Server Settings – □ ×				
Passwore	d Server Settings			
General Database	IIS Settings			
Authentication Domain Office365	Website Default Web Site V Diagnostic			
IIS Advanced	 Force https This option requires that you install an SSL certificate in IIS. Please see IIS documentation on the steps to follow. Manage Certificate ① Encrypt web.config file Web application name /dps Installation folder 			
	C:\inetpub\wwwroot\dps			
	Search property Sa	ve	Can	cel

IIS Tab

SETTINGS

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

Devolutions Password Server Cor	nsole - IIS Manager HTTPS/SSL $~~ imes$
IIS Manager HTT	PS/SSL
Default Web Site Certificate Devolutions Proxy SSL Self-Signed Certifi	cate - {0A1E491C-83CB-4E4B-94C7-9Fi ↓ Create Self-Signed Certificate
/dps ✓ Require SSL	
	OK Cancel

IIS Manager HTTPS/SSL Dialog

Certificate	Select the SSL Certificate will be use with the Devolutions Password Server instance.
Create Self-Signed Certificate	Create a self-signed certificate to be use with the Devolutions Password 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 Password Server configuration.

Devolutions Passwo	ord Server Console - Passw	ord Server Settings	—		×
Password Server Settings					
General Database Authentication Domain Office365 IIS Advanced	Advanced Token Valid Time (minutes) Data validation mode User CAL type	1440 Default Default			
	Search property	4	Save	Can	cel

Advanced Tab

SETTINGS

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 Password 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	_	×
🖸 👗 👼 📑 🦓 🎝 Import Users 🃚 🍘 🗊 🔊 📰 😂 🖁		:
Actions Details		

Devolutions Password Server Console Commands Toolbar

Refresh	Refresh the current information.
Manage Users	Manage users with the <u>User Management</u> .
Manage Security Groups	Opens the Security Group Management. (Legacy)
Manage Vaults	Opens the <u>Vault Management</u> .
Manage Roles	Opens the <u>Role Management</u> .
Import Users	Access the Import Users feature.
System Settings	Manage the <u>System Settings</u> .
System Permissions	Manage the <u>System Permissions</u> .
Security Providers	Manage the <u>Security Providers</u> .
Backup Manager	Access the <u>Backup Manager</u> feature.
View Logs	Access the <u>View Logs</u> feature.

View web client	Access the Web Interface.
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 <u>Authentication</u> topic for more information.

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

Devolutions	Password Server Console			_		\times
C 🕯 👼 🛢 -	🔓 👶 Import Users 👰 🍘 🖇	9 🗟 🕲 🗖 🛢 🔚				:
Actions	Details Import users from LDAP					
	Name	Devolutions Password Server	Version		2019.1	.9.0

Devolutions Password Server Console Commands Toolbar

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

Devolutions Password Server Console - Import Users from LDAP					
🖬 Imp	port User	s from LDAP			
	Already Crea	User Principal Name	Sam Account Nan	ne First Name	^
		5			
		Ł		1	
		Ł		1	
		c		I	
		c			
		c		(
		e		I	
		f		I	
		i.		1	
		j	:	· · · · ·	
		j	_		
		li			
<		· · · · ·			>
Administration	Credentials	🗹 Do	on't show users already crea	ted 🖸 Imp	ort Cancel

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.

8					_		Х
Backup configuration	n						
Database Advance	d						
Database Configu	iration				Save		
Enable database ba	ckup 🖂				Cancel		
Backup database file	e path \\DC\T	eamShar	e\BackupDVLS		Backup Now		
Web Configuratio	n						
Enable web backup	\checkmark						
Backup database file	e path	eamShar	e\BackupDVLS				
Schedule Notify Administrator	on backup failed						
Backup start time	2018-06-01	9:20:0	PM				
Repeat every	Days 1 🛓 Ho	urs	Minutes 0				
Start date/time	End date/time	N	Filename	Database	filename	Success	^
2018-08-02 9:22 AM			\\Rigel\Temp\Web\dvlsorion_02082018_132206		Share \BackupDVLS \Orion \dvlsorion	 Image: A second s	
2018-08-01 8:00 PM	2018-08-01 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_02082018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	 Image: A second s	
2018-07-31 8:00 PM	2018-07-31 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_01082018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	
2018-07-30 8:00 PM	2018-07-30 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_31072018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	
2018-07-29 8:00 PM	2018-07-29 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_30072018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	
2018-07-28 8:00 PM	2018-07-28 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_29072018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	
2018-07-27 8:00 PM	2018-07-27 8:01 PM	D	\\Rigel\Temp\Web\dvlsorion_28072018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	\mathbf{v}

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 Password Server

4.1.2.2.1 Database

DESCRIPTION

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

8				-		\times
Backup configuration						
Database Advanced						
Database Configuration				Save		
Fachla database hadeen				Cancel		
Enable database backup						
Backup database file path	\\DC\TeamShar	e\BackupDVLS		Backup Now		
Web Configuration						
web configuration						
Enable web backup	\checkmark					
Backup database file path	\\DC\TeamShar	e \BackupDVLS				
Schedule						
Notify Administrator on backup fa	iled					
Backup start time 2018-06-01	9:20:0	0 PM 🚖				
Repeat every Days 1	Hours	Minutes 0				
	- Hours					
Start date/time End date/tim	ne N	Filename	Database	filename	Success	^
2018-08-02 9:22 AM 2018-08-02	9:23 AM D	\\Rigel\Temp\Web\dvlsorion_02082018_132206	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	~	
2018-08-01 8:00 PM 2018-08-01	B:01 PM D	\Rigel\Temp\Web\dvlsorion_02082018_130000	\\DC\Team	Share\BackupDVLS\Orion\dvlsorion	A	
2018-07-31 8:00 PM 2018-07-31	B:01 PM D	\\Rigel\Temp\Web\dvlsorion_01082018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion	_	
2018-07-30 8:00 PM 2018-07-30	B:01 PM D	\\Rigel\Temp\Web\dvlsorion_31072018_130000	\\DC\Team	Share\BackupDVLS\Orion\dvlsorion		
2018-07-29 8:00 PM 2018-07-29	B:01 PM D	\\Rigel\Temp\Web\dvlsorion_30072018_130000	\\DC\Team	Share\BackupDVLS\Orion\dvlsorion	-	
2018-07-28 8:00 PM 2018-07-28	B:01 PM D	\\Rigel\Temp\Web\dvlsorion_29072018_130000	\/DC\Team	Share \BackupDVLS \Orion \dvlsorion	× .	
2018-07-27 8:00 PM 2018-07-27	B:01 PM D	\Rigel\Temp\Web\dvlsorion_28072018_130000	\\DC\Team	Share \BackupDVLS \Orion \dvlsorion		\checkmark

Backup Manager

SETTINGS

CONTROLS

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

Enable database backup	Activate the backup of the SQL database.
Backup database file path	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. 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.

WEB CONFIGURATION

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

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.
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	 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.

8				-		×
Backup configuratio	n					
Database Advance	d					
General				Save		
Database backup SC	OL timeout (Minutes)	1 🜲		Cancel		
	i					
Keep number of bac	xups			Backup Now		
Copy Only database	e backup	\checkmark				
Start date/time	End date/time	Notes	Filename	Database filename	Success	^
2018-08-02 8:00 PM		Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_030	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-08-02 9:22 AM	2018-08-02 9:23 AM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_020	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-08-01 8:00 PM	2018-08-01 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_020	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-07-31 8:00 PM	2018-07-31 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_010	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-07-30 8:00 PM	2018-07-30 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_310	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-07-29 8:00 PM	2018-07-29 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_300	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	
2018-07-28 8:00 PM	2018-07-28 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_290	\\DC\TeamShare\BackupDVLS\Ori	-	
2018-07-27 8:00 PM	2018-07-27 8:01 PM	Database backup completed. DVLS	\\Rigel\Temp\Web\dvlsorion_280	\\DC\TeamShare\BackupDVLS\Ori	 Image: A second s	¥

Backup Manager - Advanced

SETTINGS

GENERAL

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

8							—		×
Date	Last 7 Days	Ŧ	4/29/2019	То	5/6/2019	Ŧ			
Username									
Message			Local time	r					
Туре	All	*	Search Search	<u>n</u> m				784 Logs	
Date 👻	Title					Username		Туре	^
4/30/2019 11:42 AM	Application_Start							Information	
4/30/2019 11:42 AM	Application_End					DPS Server		Information	
4/30/2019 11:38 AM	GetPartialConnectionTree							Warning	
4/30/2019 11:38 AM	GetPartialConnectionTree							Warning	
4/30/2019 11:38 AM	t/30/2019 11:38 AM GetPartialConnectionTree				Warning				
4/30/2019 11:38 AM	/30/2019 11:38 AM GetPartialConnectionTree			Warning					
4/30/2019 11:38 AM	38 AM GetPartialConnectionTree				Warning				
4/30/2019 11:26 AM	Update Azure cache end Scheduler				Debug				
4/30/2019 11:25 AM	Update Azure cache start					Scheduler		Debug	
4/30/2019 11:06 AM	DirectoryServicesCOMExcep	otion	- The user name or passwor	d is incorrect				Debug	
4/30/2019 11:06 AM	Application_Start							Information	
4/30/2019 11:05 AM	Application_End					DPS Server		Information	
4/30/2019 11:04 AM	Application_Start Information				~				
DirectoryServicesCOMException - The user name or password is incorrect. at System.DirectoryServices.DirectoryEntry.Bind(Boolean throwIfFail) at System.DirectoryServices.DirectoryEntry.Bind() at System.DirectoryServices.PropertyValueCollection.PopulateList() at System.DirectoryServices.PropertyValueCollectionetor(DirectoryEntry entry, String propertyName) at System.DirectoryServices.PropertyCollectionetor(DirectoryEntry.Bind) at System.DirectoryServices.PropertyCollection.get_Item(String propertyName) at System.DirectoryServices.AccountManagement.PrincipalContext.DoLDAPDirectoryInitNoContainer()									
1									/

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

Devolutions Password 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 Password Server instance is located on the computer.

📙 🛃 📊 🖛 dv	/ls			_	
File Home	Share View				~ 🕐
$\leftarrow \rightarrow \cdot \uparrow$	« Local Disk (C:) > inetpub > www.ro	ot > dvls >	✓ Ö Sea	arch dvls	م
A Duic	Name	Date modified	Туре	Size	
	App_Data	2018-03-19 8:42 AM	File folder		
	Areas	2018-02-06 2:12 PM	File folder		
	📙 bin	2018-03-19 8:42 AM	File folder		
≝ I <i>★</i>	client	2018-02-06 2:12 PM	File folder		
📰 l 🖈	Custom	2018-02-06 2:12 PM	File folder		
This	DBScripts	2018-02-06 2:12 PM	File folder		
		2018-02-06 2:12 PM	File folder		
T C o	Scripts	2018-02-06 2:12 PM	File folder		
🛨 D o		2018-02-06 2:12 PM	File folder		
E. Des	🚹 favicon.ico	2016-08-30 11:00	lcon	49 KB	
🖆 Doc	🛤 favicon.png	2016-09-18 10:52	PNG image	1 KB	
🕹 Dov	📄 Global.asax	2015-01-18 3:34 PM	ASAX File	1 KB	
E ou	ImageBytes.ashx	2016-10-17 7:36 PM	ASHX File	1 KB	
h Mu	📄 index.aspx	2017-11-13 4:25 PM	ASPX File	3 KB	
	📄 robot.txt	2013-03-15 3:51 PM	Text Document	1 KB	
Pict	ServerInfo.ashx	2015-11-11 11:24	ASHX File	1 KB	
Vid 🗸	web.config	2018-03-19 9:55 AM	CONFIG File	9 KB	
17 items					

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 Password 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 <u>before</u> performing **Index Maintenance** or **Optimize** operation.

Devolutions Pa	Devolutions Password Server Console - Pack Data Source ×							
😂 🛛 Pack I	Data Soui	ce						
Processing	0 of 0							
Optimized entries	0	Space s	aved 0					
ID		Name		Metadata	Message			
Index Maintenance	e V	ault	Default	•	Optimize All	Optimize	Analyze	Close

Pack Data Source Dialog

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.

SETTINGS

INDEX MAINTENANCE

Devolutions Password Server Console - Pack Data Source ×						
😂 Pack Data Sour	ce					
Processing 0 of 0						
Optimized entries 0	Space saved 0					
ID	Name	Metadata	Message			
Rebuilding database indexes Update statistics C1_ConnectionHiandbookHistory_Connecti C1_ConnectionHistory_HistoryType_Versio IX_ConnectionHistory_Version IX_ConnectionLog_ConnectionID IX_ConnectionLog_UserInfoID IX_ConnectionLog_UserInfoID IX_ConnectionLog_UserInfoID	onID on_with_indudes					
Index Maintenance Va	ault Default	▼ 0;	otimize All	Optimize	Analyze	Close

Index Maintenance - Pack Data Source Dialog

ANALYZE/OPTIMIZE

Devolutions Password Server	Devolutions Password Server Console - Pack Data Source					
😂 Pack Data Soui	🤤 Pack Data Source					
Processing 11 of 11 Optimized entries 0	Space saved 0					
ID	Name	Metadata	Message			^
146F841A-C232-4A20-8A57-CE4D6 149FBF35-E474-4293-905E-C40F92 2CCDBD0B-7612-464C-9BB9-5F6796	Default Direct RDS with Gateway SSH					
33C65345-BD61-46D1-89AC-DF4AF 6F0D730A-1D72-4823-8A3D-C75A6 87CBB892-90C2-4C46-81C4-B087DF 986252DF-6C16-47E6-929D-78EF86	QA-VDOWNDVLS [Root] Administrator Test					=
B6C49A03-E033-4CA1-B21B-ECCBE	Downhill user					_
DB112C8B-4749-435C-AA3A-BA95E	bill Gateway					
E1D2A37D-78AE-4882-0607-34EC6E	Cloud Zope					~
Loading raw data Analyzing [Cloud Zone] (fd2a37d-78af-4b82-9607-34fc6e5df8b8) Analyzing [Sh1] (2ccdbd0b-7612-464-9bb9-5f67959c404) Analyzing [Test] (986252df-6c16-47f6-929d-78ff8679F2f3) Analyzing [Idi Gateway] (db112c8b-4749-435c-a3a3-ba95e930f8ac) Analyzing [Direct RDS with Gateway] (149fbf35-e474-4293-905e-c40f92fe7291) Analyzing [Direct RDS with Gateway] (149fbf35-e474-4293-905e-c40f92fe7291) Analyzing [RD Gateway] (143560f-67c9-4cc-8b07-c5580e1dab7a) Analyzing [IDirect RDS with Gateway] (149fbf35-e474-4293-905e-c40f92fe7291) Analyzing [IDirect RDS with Gateway] (149fbf35-e474-4293-905e-c40f92fe7291) (Idirect RDS with Gateway] (149fbf35-e474-4293-905e-c40f92fe7291) (Idirec						
Index Maintenance V	ault Default	-	Optimize All	Optimize	Analyze	Close
	Default Help Desk Service Desk					

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.

lacksquare Devolutions Password Server Console - Devolutions Password Server $ imes$				
Devolutions Password Server Console				
Language Ask confirmation on applicati	English 🔹			
	OK Cancel			

Options Dialog

SETTINGS

Language	Select the language of the Devolutions Password Server Console.
	Language available :
	• English
	Chinese (Simplified) Legacy
	Chinese (Traditional, Taiwan)
	• Dutch
	• French

	• 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 Password Server.

Devolutions P	assword Server Console			_		×
	🛔 🎝 Import Users 🏽 🍖 🍞	s () 🖬 🛢 🔚				1
Actions	Details		-	Check Prerequisi	ites	
	Name	Devolutions Password Server	v 🖻	Database Diagno	ostic	
	Description			Send Diagnostic	to Support	
Edit	beschpton			View Installation	Logs	
	Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-ENVTY	PI	Open Backup Fo	lder	
+			0	Manage Encrypt	ion Keys	
New			۰	Check for Updat	es	
			0	About		
×	Website	Default Web Site	Web a	pplication	/dps	
Delete	Default path	C:\inetpub\wwwroot\dps				
:	Application pool	dps	Runtii	me version	v4.0	
	Authentication	Domain, DVLS Custom				
R()	Scheduler service	Running				
Upgrade Server				Go Offline		
o ^o			<u></u>			
Uninstall Scheduler						
2019.1.9.0						

Advanced Menu

4.1.3.1 Check Prerequisites

DESCRIPTION

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

SETTINGS

Devolutions Pa	assword Server Console		– 🗆 X
	👌 🖏 Import Users 🌷 🍞 🗐	S 🖬 🛢 🔚	
Actions	Details		Check Prerequisites
	Name	Devolutions Password Server	V Database Diagnostic
	Description		Send Diagnostic to Support
Edit			View Installation Logs
	Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-ENVTY	Open Backup Folder
+			Manage Encryption Keys
New			Check for Updates
			About
X	Website	Default Web Site	Web application /dps
Delete	Default path	C:\inetpub\wwwroot\dps	
:	Application pool	dps	Runtime version v4.0
	Authentication	Domain, DVLS Custom	
R.O	Scheduler service	Running	
Upgrade Server			Go Offline
o°			
Uninstall Scheduler			
2019.1.9.0			

Options Menu

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

Devolutions Password Server Console - IIS Features Diagnostic	×
IIS Features Diagnostic	
Feature	
HTTP Errors	~
HTTP Logging	1
Static Content	~
Default Document	 Image: A second s
Directory Browsing	~
Application Initialization	 Image: A second s
ASP.NET 4.7	~
ISAPI Extensions	 Image: A second s
ISAPI Filters	~
Basic Authentication	 Image: A second s
Static Content Compression	~
Windows Authentication	- 🚸
IIS Rewrite Module	~
C O Install Prerequisites	lose

IIS Features Diagnostic

The **Install Prerequisites** button will run a PowerShell script to install the missing prerequisites. Please see <u>Installing Web Roles prerequisites</u>.

4.1.3.2 Database Diagnostic

DESCRIPTION

The **Database Diagnostics** will display information of the database health. Please contact the support team at <u>ticket@devolutions.net</u> 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

Devolutio	Devolutions Password Server Console - Database Diagnostics				\times		
🕂 Da	atab	ase Diagi	nostics				
Summary	Size	Deserialization	Duplicate Folders	Encryption	Virtual Folders		
Session dese	erializati	ion			~		
Session encr	yption				~		
Duplicate gro	oups				~		
						Clos	se

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 Password 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**.

Devolutions P	assword Server Console		– 🗆 ×	<
	🖁 🎝 Import Users 🏽 🍖 🍞 🛙	ā (\$ 🖬 🛢 🔚		÷
Actions	Details		Check Prerequisites	
	Name	Devolutions Password Server	v Database Diagnostic Send Diagnostic to Support	
Edit	Description Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-ENVTY	View Installation Logs Pl Open Backup Folder	
+			Manage Encryption Keys	
New			Check for Updates	
X	Website	Default Web Site	Web application /dps	
Delate	Default path	C:\inetpub\wwwroot\dps		
Delete	Application pool	dps	Runtime version v4.0	
	Authentication	Domain, DVLS Custom		
RU	Scheduler service	Running		
Upgrade Server			Go Offline	
o°				
Uninstall Scheduler				
2019.1.9.0				

Advanced Menu

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

Devolutions Passwo	ord Server Console - Send Message to Devolutions Support Team	×
📥 Send Me	essage to Devolutions Support Team	
Personal Information		
Email	YourEmail@YourDomain.com	
Company	Your Company	
Name	Your Name Here	
Subject		
Message	1	
		^
<		>
Save to File	ОК	Cancel

Send Diagnostic Report Dialog

SETTINGS

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.

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 Password Server instance.

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

Devolutions Page 1	assword Server Console			– 🗆 X
	👌 🕹 Import Users 🏽 🍖 🍞 🛙	ā 🕲 🖬 🛢 🔚		:
Actions	Details		_	Check Prerequisites
	Name	Devolutions Password Server	v 🖬	Database Diagnostic
	Description			Send Diagnostic to Support
Edit	Description			View Installation Logs
	Serial (server)	XXXXX-XXXXXX-XXXXX-XXXXX-ENVTY	PI	Open Backup Folder
+			0	Manage Encryption Keys
New				Check for Updates
			0	About
X	Website	Default Web Site	Web a	pplication /dps
Delete	Default path	C:\inetpub\wwwroot\dps		
:	Application pool	dps	Runtii	me version v4.0
	Authentication	Domain, DVLS Custom		
RU	Scheduler service	Running		
Upgrade Server				Go Offline
0 ⁰				
Uninstall Scheduler				
2019.1.9.0				

Advanced Menu

Iog.txt - Notepad \times 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**.

Devolutions P	assword Server Console			_	- 🗆	×
	🔰 🕹 Import Users 🏽 🍖 🍞 🗐	J (S) 🖪 🛢 🔚				:
Actions	Details		-	Check Prerec	uisites	
	Name	Devolutions Password Server	v 🖬	Database Dia	gnostic	
	Description			Send Diagno	stic to Suppo	rt
Edit				View Installat	ion Logs	
	Serial (server)	XXXXX-XXXXX-XXXXX-XXXXX-ENVTY	PI Si	Open Backup	Folder	
-			0	Manage Encr	yption Keys	
New			۹	Check for Up	dates	
			0	About		
	Website	Default Web Site	Web a	pplication	/dps	
Delete	Default path	C:\inetpub\wwwroot\dps				
:	Application pool	dps	Runtir	me version	v4.0	
	Authentication	Domain, DVLS Custom				
R()	Scheduler service	Running				
Upgrade Server				Go Offline		
o ^o			<u></u>			
Uninstall Scheduler						
2019.1.9.0						

Advanced Menu

📙 🛃 📑 🖬 🖛 D	IVLS		- 0	×
File Home	Share View			~ 🕐
$\leftarrow \rightarrow \land \uparrow$	🛶 « AppData > Local > Temp > DVLS >	✓ Ö Search	DVLS	Q
🔮 Docume ^	Name ^	Date modified	Туре	Size
🕂 Downlo	2018-06-313-49	2018-03-06 1:49 PM	File folder	
🛖 E on DE'	2018-06-313-50	2018-03-06 1:50 PM	File folder	
👌 Music	2018-13-310-36	2018-03-13 10:36	File folder	
Pictures	2018-14-309-47	2018-03-14 9:48 AM	File folder	
😽 Videos	2018-14-314-50	2018-03-14 2:50 PM	File folder	
🏪 Local Di	2018-19-314-03	2018-03-19 2:03 PM	File folder	
	🔄 Install	2018-03-19 2:04 PM	File folder	
	📄 log.txt	2018-03-19 2:04 PM	Text Document	
💣 Network				
~	<			>
8 items				

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 Password Server.

Devolutions P	assword Server Console			– 🗆 X
	🛔 🎝 Import Users 🏽 🍖 🍞 🖡	s () 🖬 🛢 🔚		:
Actions	Details		-	Check Prerequisites
	Name	Devolutions Password Server	v 🖻	Database Diagnostic
	Description			Send Diagnostic to Support
Edit				View Installation Logs
	Serial (server)	XXXXX-XXXXXX-XXXXXX-ENVTY	PI	Open Backup Folder
+			O	Manage Encryption Keys
New			۹	Check for Updates
			0	About
X	Website	Default Web Site	Web a	pplication /dps
Delete	Default path	C:\inetpub\wwwroot\dps		
:	Application pool	dps	Runtii	me version v4.0
	Authentication	Domain, DVLS Custom		
RUS	Scheduler service	Running		
Upgrade Server				Go Offline
o ^o				
Uninstall Scheduler				
2019.1.9.0				

Advanced Menu

\fbox Devolutions Password Server Console - Manage Encryption Ke $\qquad \times$		
🚹 Mana	age Encryption Keys	
Web Application —		_
Operation	Export ~	
	🗸 Login Key	
	☑ Token Storage Key	
	_	
	Security provider configuration	
Password	•	
	OK Cance	1

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 Password Server is deployed in a High Availability or Load Balancing topology, the encryption keys must be the same on all Devolutions Password Server instances connected on the same SQL database.

Operation	 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 Password Server for logins.
Token Storage Key	The encrypted key used by Devolutions Password Server for the token.
Security provider configuration	The encrypted key used by Devolutions Password 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.

Devolutions P	assword Server Console			_		\times
	🛔 🎝 Import Users 🏽 🍖 🍞) 🗔 🕲 🖪 🛢 불				:
Actions	Details		-	Check Prerequisi	tes	
	Name	Devolutions Password Server	v 🖬	Database Diagno	stic	
	Description			Send Diagnostic	to Support	
Edit	Description			View Installation	Logs	
	Serial (server)	XXXXX-XXXXXX-XXXXXX-XXXXXX-ENVTY	Pl	Open Backup Fo	lder	
+			°	Manage Encrypti	on Keys	
New			٩	Check for Update	es	
			0	About		
×	Website	Default Web Site	Web a	pplication	/dps	
Delete	Default path	C:\inetpub\wwwroot\dps				
i	Application pool	dps	Runtin	ne version	v4.0	
	Authentication	Domain, DVLS Custom				
K()	Scheduler service	Running				
Upgrade Server				Go Offline		
o						
Uninstall Scheduler						
2019.1.9.0						
		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.

Devolutions Pa	assword Server Console				_ 🗆	×
	🔰 👶 Import Users 🏽 🍖 🛸 🖉) 🗟 🕄 🗖 🛢 🔚				:
Actions	Details		_	Check Prere	equisites	
	Name	Devolutions Password Server	v 🖻	Database Di	iagnostic	
	Description			Send Diagn	ostic to Support	
Edit				View Install	ation Logs	
1. A.	Serial (server)	XXXXX-XXXXX-XXXXX-ENVTY	PI	Open Backı	up Folder	
+			Ø	Manage En	cryption Keys	
New			۲	Check for U	pdates	
			0	About		
X	Website	Default Web Site	Wev a	pplication	/dps	
Delete	Default path	C:\inetpub\wwwroot\dps				
:	Application pool	dps	Runtin	ne version	v4.0	
	Authentication	Domain, DVLS Custom				
R ()	Scheduler service	Running				
Upgrade Server				Go Offline		
o°						
Uninstall Scheduler						
2019.1.9.0						

Advanced Menu

Devolutions Password Server Console ×		
About Devolutions Password Server Console		
Devolutions Password Server Console En	terprise Edition	
Devolutions inc.	.NET Runtime: v4.0.30319	
Copyright © 2006-2019		
Version 2019.1.9.0	Current user WINDJAMMER (David	
	Loaded Add-Ons Open Source	
https://devolutions.net	Name 🔺 Type	
https://server.devolutions.net		
License information		
Memory usage		
151 MB		
	I	

About Dialog

4.2 Authentication

DESCRIPTION

Devolutions Password Server supports multiple authentication modes.

Devolutions Passwor	d Server Console - Password Server Settings	-		×
Password	d Server Settings			
General Database Authentication Domain Office365 IIS Advanced	Authentication Modes ✓ Authenticate with domain user Authentication with database [Deprecated] ✓ Authenticate with Office 365 user Authenticate with local machine user [Deprecated] ✓ Authenticate with local machine user [Deprecated] ✓ Authenticate with Devolutions Password Server custom user Windows Authentication ✓ Enable Windows authentication ✓ Windows authentication requires further configuration on your IIS server. Pleatele button for instructions.	se dick the	3	
	Search property	Save	Cance	el

Authentication Tab

SETTINGS

AUTHENTICATION MODES

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

WINDOWS AUTHENTICATION

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

AUTOMATIC USER ACCOUNT CREATION

When using authentication modes other then **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 Password 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 then 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 <u>Root Settings</u> 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 Password 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.

- <u>User Management</u>
- <u>Role Management</u>

- Vault Management
- 4.3.1 User Management

DESCRIPTION

Users

igation



🔁 Dashboard

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 Password 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 Remote Desktop Manager

л х

Management

Devolutions Password Server Console - User and Security Management							
User and Security Management							
Management	🕂 Add User 🛛 🖋 💽 🗙 💷	🂵 👧 🕽 🕽 Filter					
Users	Login	Name	User type	Authentication Type			
Security Groups				Custom (Devolutions)			
Repositories	lisa.andrews@orion.loc	Lisa Andrews	User	Domain			
Roles	trent.baker@orion.loc	Trent Baker	Restricted user	Domain			
Reports	william.fox@orion.loc	William Fox	User	Domain			
User Locked							
				/			
Yiew History	Administration Credentia	ls		Close			

Users Management Dialog

SETTINGS

CREATE USERS

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

Devolutions Server Con	Devolutions Server Console - User and Security Management				
🧊 User and	d Security	Management			
Management	🕂 Add User	🗶 💷 🔬 🗲 Filter			
Users	Login	A Name	User type	Authentication Type	
Security Groups	Add User				
Repositories					
Roles					
Reports					
User Locked					
	<			>	
View History				Close	

User Management - Add User

USER MANAGEMENT SETTINGS

GENERAL

Devolutions Password Server Console - User Management					
🔓 User Manag	ement				
General ▷ Information Roles Privileges Security Groups Vaults Application Access Settings Email Notifications	General ID Authentication type Username Password User type User license type Information First name Email	SC68ADAB-F88E-42F5-A791-697844D4DDB5 Custom (Devolutions) User User User User User Senabled Default User must change password at next logon Send user an email invite Last name			
·	L	ОК	Ca	ncel	

User Management - General

Authentication type	Select the user's authentication type:
	• Custom (Devolutions): create a user specific to Devolutions Password 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.
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: 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.

Devolutions Password	Server Console - Use	r Management				×
🔓 User Mana	agement					
General Information Roles Privileges Security Groups Vaults Application Access Settings Email Notifications	Information Company Job title Department Gravatar email Language	English				
				ОК	Ca	ncel

User Management - Information

ROLES

Select roles to assign to the user.

Devolutions Password Se	Devolutions Password Server Console - User Management			
🔓 User Manag	ement			
General > Information	Roles			
Roles	Name 🔺	Description	Is Member	
Privileges	CustomRole			
Security Groups	Show-Corporate			
	Show-Help Desk			
Settinas	Show-IT Corp			
Email Notifications	Show-Mkt			
	WINDJAMMER \RDM Help Desk			
	WINDJAMMER \RDM Service			
		0	K Cancel	

User Management - Roles

Roles	Check the Is Member box to assign the role to the user. Consult <u>Role Management</u> topic for more information.

PRIVILEGES

Devolutions Password Se	Devolutions Password Server Console - User Management				
🎖 User Manag	ement				
General Information Roles Privileges Security Groups Vaults Application Access Settinge	General View information section Activity logs	Allow 💌			
Email Notifications	Import / Export Import Export	Allow T			
	L		OK Cancel		

User Management - Privileges

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

SECURITY GROUPS (LEGACY)

The Security Groups section manages permissions with Security Groups.

<u>We do not recommend using this method</u>, it is now considered a <u>Legacy</u> setting and is best replaced by the <u>Role Management</u>.

Devolutions Password Se	erver Console - User Management		×
🔓 User Manag	ement		
General ▷ Information Roles	Security Groups		
Privileges Security Groups	Name Has Access		
Vaults Application Access Settings Email Notifications			
	OK	Car	ncel

User Management - Security Groups

VAULTS

Select which Vaults the user has access to.

Devolutions Password S	Devolutions Password Server Console - User Management				
🔓 User Manag	gement				
General	Vaults				
Information Roles	Name		Description		Allow
Privileges	Default				✓
Security Groups	Help Desk				
Application Access	Service Desk				
Settings					
Email Notifications					
				Select All	Unselect All
					K Cancel
					Cancel

User Management - Vaults

APPLICATION ACCESS

Select which application the user will be allowed to use.

Devolutions Password S	Server Console - User Manager	nent				×
🔓 User Manag	gement					
General ▷ Information Roles	Application Access Remote Desktop Manager	Allow	T			
Privileges Security Groups Vaults	Devolutions Web Login Devolutions Launcher	Allow	v			
Application Access Settings Email Notifications	Web	Allow	¥			
L				ОК	Car	ncel

User Management - Application Access

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

SETTINGS

Allow the user to enable the <u>Offline Mode</u> and whether or not they can use the Drag-n-Drop feature.

Devolutions Password S	Devolutions Password Server Console - User Management			×
🔓 User Manag	gement			
General Information Roles Privileges Security Groups Vaults Application Access Settings Email Notifications 	Settings Offline mode Allow drag-and-drop	Read-only		
		OK	Ca	ncel



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.

Devolutions Password Se	rver Console - User Management				×
🔓 User Manag	ement				
General ▷ Information Roles Privileges Security Groups Vaults Application Access Settings Email Notifications	Email Notifications Connection opened Data Source Settings changed Entries Vault Roles Security groups Tasks Users Users Users Users Entry expiring Watched By	30 days	15 days	5 days	
	Username _administrator bill@windjammer.loc david@windjammer.loc ellen@downhillpro.xyz		On Edit On Edit On Edit On Edit On	On Delete	*
				ОК Са	ancel

User Management - Email Notifications

4.3.2 Role Management

DESCRIPTION



Roles in Devolutions Password Server are mainly used to <u>reduce the time taken to</u> <u>manage users</u>. 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 Password Server. Once a domain user logs in the Devolutions Password Server data source, their user account will be created if needed and users rights will be controlled by the defined groups.

Devolutions	Password Server Console
C 🕴 🎘 🖥	👪 🎝 Import Users 🐞 🎓 😎 🖍 🕾
Actions	Details Roles

Manage Roles in Devolutions Password Server Console

🗳 🕂	/ ၁	Quid	k Connect	<host></host>	
FILE	HOME	EDIT	VIEW	ADMINISTRATIO	DN TOOLS
-	P				:
Users	Security Groups	Repositories	Roles	Root (Settings)	Reports Da
		Manageme	ent	-	
Na	vigation		Roles] # × 🙆	Dashboard

Manage Roles in Remote Desktop Manager

Devolutions Password	Devolutions Password Server Console - User and Security Management		
🧊 User an	d Security Management		
Management	🕂 Add Role 📝 🎲 🗙 💭 Filter		
Users	Name Description		
Security Groups	ORION\Team A		
Repositories			
Reports			
User Locked			
Yiew History	Administration Credentials		Close

Roles Management Dialog

SETTINGS

CREATE ROLES

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

Devolutions Password S	🕻 Devolutions Password Server Console - User and Security Management – 🗆 🗙				
🧊 User and	Security Management				
Management	🕂 Add Role 🥒 🎲 🗙 💭 Filter				
Users	Name Description				
Security Groups	Add Role				
Repositories					
Roles					
Reports					
User Locked					
View History			Clo	se	

Role Management - Add Role

ROLE MANAGEMENT SETTTINGS

GENERAL

Devolutions Password S	Devolutions Password Server Console - Role Management				
🔏 Role Mana	gement				
General Privileges Security Groups Vaults Users Email Notifications	General ID 5C565F4D-8155-4306-8EAC-2C82678EEFD7 Name Description Administrator				
		OK Cancel			

Role Management - General

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 Password Server.

VAULTS

Devolutions Password Server Console - Role Management					
🔒 Role Manag	ement				
General	Vaults				
Privileges					
Security Groups	Name	٠	Description		Allow
Vaults	Default				✓
Users	Help Desk				
Email Nouncations	Service Desk				
				Select All	Unselect All
				OK	Cancel

Role Management - Vaults

Vaults	Consult the Vaults topic for more information.

USERS

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

Devolutions Password Server Console - Role Management			×		
🚷 Role Manag	ement				
General Privileges Security Groups	Name 🔺	Description	Administrator	Is Member	
Vaults	bill@windjammer.loc	Bill Preston			
Users	david@windjammer.loc	David			
Email Notifications	ellen@downhillpro.xyz	Ellen Adams			
	erica.poirier@downhillpro.xyz	Erica Poirier			
			ОК	Can	cel

Role Management - Settings

EMAIL NOTIFICATIONS

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

Devolutions Password Server Console - Role Management			\times		
🚷 Role Manag	gement				
General Privileges	Watched By				
Security Groups	Username		On Edit	On Delete	
Vaults	_administrator				
Users	bill@windjammer.loc				
Email Notifications	david@windjammer.loc				
	ellen@downhillpro.xyz				
	erica.poirier@downhillpro.xyz				
			ОК	Can	cel

Role Management - Email Notifications

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

Devolutions Password Server Console - Role Management			×	
🔒 Role Mana	agement			
General Privileges Security Groups Vaults Users Email Notifications	General View information section Activity logs	Default v		
	Import / Export Import Export	Default		
			ок с	ancel

Role Management - Privileges

View information section	Allows the user to see the content of the <u>Information</u> tab for all sessions.

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

SECURITY GROUPS

Devolutions Password	Server Console	e - Role Management		\times
🚷 Role Mana	agement			
General	Rights			
Privileges				
Security Groups	Add	Default		
Vaults	Edit	Default 🔻		
Email Notifications	Delete	Default 🔻		
	Security Grou	ups		
	🗸 Use sin	nplified security		
	Name	Has Access		
l				
		ОК	Ca	ncel

Rights	Allows Add, Edit and/or Delete rights or blocks Add in root right.
Security Groups	To learn more about Permissions please see the <u>System</u> <u>Permissions</u> 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 in Remote Desktop Manager

Devolutions Passwo	rd Server Console - User and Security Management	
🕥 User and	Security Management	
Management	+ Add Vault 🕜 🛔 🍓 🗙 😅 Filter	
Users Security Groups	Image Name 🔺 Description	Allow offline
Vaults	Oefault Default	✓
Roles	Help Desk	✓
Reports	Service Desk	✓
View History	Administration Credentials	Close

Vaults Management Dialog

SETTINGS

CREATE VAULTS

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

Devolutions Passw	rord Server Console - User and Security Management	
🕥 User and	d Security Management	
Management	+ Add Vault 🖋 🕯 🍇 🗶 🗯 Filter	
Users Security Groups	Image Name Description	Allow offline
Vaults	😝 Default	✓
Roles	Help Desk	✓
Reports	Service Desk	✓
View History	Administration Credentials	Close

Vaults Management - Add Vault

VAULT MANAGEMENT SETTINGS

GENERAL

Devolutions Password Server Console - Vault Management			\times	
🗧 Vault Man	agement			
General Users Roles Email Notifications	General ID Name	E0CC0E25-41A6-40B3-BD56-F4CEEFF1733B		
	Description			^
		Allow offine	Car	ncel

Vault Management - General

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 <u>Offline Mode</u> .

USERS

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

Devolutions Password Server Console - Vault Management				\times	
📕 Vault Man	agement				
General Users	Name	Description	Administrator	Is Member	
Roles	_administrator		1	✓	
Email Notifications	bill@windjammer.loc	Bill Preston			
	david@windjammer.loc	David			
	ellen@downhillpro.xyz	Ellen Adams			
	erica.poirier@downhillpro.xyz	Erica Poirier			
			ОК	Cance	1

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.

Devolutions Password Server Console - Vault Management			×		
🗧 Vault Mana	gement				
General Users	Name 🔺	Description	Administrator	Is Member	
Roles	CustomRole				
Email Notifications	Show-Corporate				
	Show-Help Desk				
	Show-IT Corp				
	Show-Mkt				
	WINDJAMMER \RDM Help Desk				
	WINDJAMMER \RDM Service Desk				
			ОК	Cancel	

Vault Management - Roles

EMAIL NOTIFICATIONS

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

Devolutions Password Server Console - Vault Management				\times
🚍 Vault Mana	gement			
General Users	Watched By			
Roles	Username	On Edit	On Delete	
Email Notifications	_administrator			
	bill@windjammer.loc			
	david@windjammer.loc			
	ellen@downhillpro.xyz			
	erica.poirier@downhillpro.xyz			
		ОК	Cance	el

Vault Management - Email Notifications

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 Password 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 V

5 Web Interface

DESCRIPTION

The Devolutions Password Server web interface offers a simplified interface for endusers to use and manage passwords from any web browser.

LOGIN PAGE

Open a web browser and navigate to the URL of the Devolutions Password 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 Password Server account to connect.

Log in	volutions ssword Server
Username	*
Password	*
	Log In v 2019.1.20.0

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.

Pevolutions Password Server
🙆 Dashboard
🛞 Vaults
🍙 My Private Vault
O Search
☆ Favorites
Reports
Administration
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**.

Pevolutions Password Server			🚾 Windja	ammer Defa	. *			区 (
Dashboard	DASHBOARD							Change landing page
Vaults	My Check Outs				ान्तु My Activity Logs			
🚯 My Private Vault	Name ¢				Connection ¢	Message		Vault
Search					MS Office	Viewed entry	15 days ago	Windjammer IT Vault
Favorites		No data to disp	blay		MS Office	Viewed entry	15 days ago	Windjammer IT Vault
Reports					RD Gateway Password	Password viewed	15 days ago	Windjammer IT
Administration	Expired Entry List			¢	RD Gateway Password	Viewed entry	15 days ago	Windjammer IT
-	Name ¢	Since	Vault		RD Gateway Password	Exported entry (Native)	15 days ago	Windjammer IT
	No data to display		Talent	Exported entry (Native)	15 days ago	Windjammer IT		
			RDS with Broker	Exported entry (Native)	15 days ago	Windjammer IT		
					Direct RDS with Gateway	Exported entry (Native)	15 days ago	Windjammer IT
	✓ All vaults				Talent	Entry created	15 days ago	Windjammer IT
	My Vaults				RD Gateway	Viewed entry	15 days ago	Windjammer IT
	Name ©					8 € 1 2	3 F N	25 Results
	Downhill Pro				All vaults			
	Telemark							
	Windjammer Corp							
	Windjammer Default							
	Windjammer IT							
2019.2.1.0	Windjammer IT Vault							

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 Password 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 Acc	ount	2 × 🖸
INFORMATION	▼ GENERAL	
	First name	Last name
	Email administrator@windjammer.net	Company
	Language English	
	 ADDRESS 	
	Address	State
		Country Select 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.

Change your avatar	🛛 🗙
Gravatar email	
Leave blank to use the default avatar. If you don't have a Gravatar, get one at gr	avatar.com
SAVE	CANCEL

Change your Avatar

CHANGE PASSWORD

Allow the user to modify his password. Only available for Devolutions Password Server Custom or Database account type. Please see <u>Authentication</u> for more information.

Change Password	2 ×
Current password	Ø
New password	;
Confirm Password	•
	SAVE CANCEL



SETTINGS

Modify User Interface elements.

Settings	2 ×
Landing page Vaults	•
Launch connection with Devolutions Launcher	-
Grid page size 10	
Date and time format Default	-
	SAVE CANCEL

User Interface Settings

Landing page	Choose the home page that opens when you sign on: • Dashboard • Vaults • My Private Vault
	Reports
	Administration
Launch connection with	 Choose the application that opens remote connections: Default: refers to Devolutions Launcher Remote Desktop Manager Devolutions Launcher

Grid page size	Choose the number of rows displayed in lists (e.g. reports)10		
	• 20		
	• 30		
Date and time	Choose a format:		
	 Default: month/day/year 		
	• US		
	Custom		

USER INFORMATION

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

User Information			×
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	Vac		~
Ĩ		CLC)SE

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		
myemail@mydomain.com		
Company		
My Company		
Name		
My Name		
Send data source information		
 Diagnostic information 		
MESSAGE		
Subject		
Detail		
	_	
	SEND TO SUPPORT 🔻 CAN	ICEL
	Download the Zip	

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

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 <u>create entries</u> 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.

🐻 Windjammer IT 🗸 🗸				⊠			
in-house			Þ A	1	101	3 E	
 Wault (Windjammer (T) Credentials O coman Tools Cood Zone 	RDM Agents Microsoft Remote Deskto OVERVIEW DOCUMENTATION	0(809) i attachments logs enterhistory				¢ G	ł
	HOST	192.168.1.105 david					
Kypervisors Sync Root	PASSWORD	•••••				©Ũ	;
RDM Agents Wark	OPEN CONSOLE (ADMIN MODE)	No					
internal Tools for Third Party	TAGS	agent windjammer12 script					
 Tools 							
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

>	* >	
Vault (Default)	🚞 Cloud Zone	– FOLDERS (2)
Cloud Zone RD Gateway	 Default QA-VDOWNDVLS 	Cloud Zone Default Folder
Administrator bill Gateway Direct RDS with Gateway	SSH	– ENTRIES (2)
Direct NDS with Gateway P Downhill user QA-VDOWNDVLS		QA-VDOWNDVLS RDP (Microsoft Re SSH Shell
Default Ø QA-VDOWNDVLS		
👳 SSH		
•	•	•
		V

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

DASHBOARD

				€			÷	Е
QA-V Microso	DOWNDVLS	op (RDP)					*	\bigcirc
OVERVIEW	DOCUMENTATIO	N ATTACHME	NTS	LOGS	ENTRY H	IISTORY		
	HOST	QA-VDOWNDVL	S.downh	ill.loc				
	USERNAME	administrator						
	DOMAIN	downhill						
	PASSWORD	•••••						⊕ [ੈ
OPEN CONSOLE	(ADMIN MODE)	No						

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

Entry Overview

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. User Specific Settings Save as Template View Password History

	• 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 <u>only they</u> <u>can access, not even an administrator could access them</u>. The **Private Vault** prevents users from using a non-secure tool to manage their personal passwords at work.

Devolutions Password Server		MPY My Private Vault 🗸 🗸	
Dashboard	 		O E
 Vaults My Private Vault 	Private Vault Downhill Telemark	Private vault	
 Q Search ☆ Favorites 	 Windjammer Co.Card Implement of the second seco		
Reports			
2019.1.20.0	•		

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 Password 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.

Add New Entry		2 ×
 Entry Session Information Contact Document Folder Credential Entry Template Import 	Search> Image: Alarm Codes Image: Bank Account Image: Command Line (External Application) Image: Company Image: Contact Image: Contact Image: Contact Image: Data Source Configuration (.rdd) Image: Device (router, switch, firewall,)	 Apple Remote Desktop (ARD) Certificate Company Connection String Credit Card Customer Database Document
		CONTINUE CANCEL

New Entry

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	<u>Contact</u> 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	<u>Credential</u> 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 form credential entries) and can be used in a variety of ways.

Add New Entry		2 ×
👻 🛅 Entry	<search></search>	
Session	Apple Remote Desktop (ARD)	Command Line (External Application)
Contact	FTP	Host
Credential Entry	Microsoft RDP Gateway	Proxy Tunnel (HTTP, SOCKS4, SOCKS4A, SOCKS5)
and Import	RDP (Microsoft Remote Desktop)	SCP SCP
	FTP	SSH Port Forward
	SSH Shell	SSH Tunnel
	TFTP	TeamViewer
	Telnet	VMware (Player, Workstation, vSphere) v
		CONTINUE CANCEL

Add a New Session Entry

5.3.2.1.1 RDP (Microsoft Remote Desktop)

DESCRIPTION

GENERAL

RDP (Microsoft F	Remote Desktop)	×	
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	 ✓ GENERAL Enter the name of the remote computer Computer ● Host Port 3389 ● Default port RDP type Normal ● Username Domain Password ● Password ● Compute and a second and a s		~
	ADD 0	L	

RDP (Microsoft Remote Desktop) - General

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: Normal Azure Cloud Services

	• 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 I	Remote Desktop)		2	×
GENERAL MORE	✓ DISPLAY			^
SECURITY	Remote Desktop Size			
USER INTERFACE	Remote Desktop Size			
EMAIL	Default 🗸	Center on screen		
NOTIFICATIONS	Custom width	Custom height		
ADVANCED	0	0		
	Screen sizing mode			
	Default	~		
	Span on multiple screens if possible			
	Use all my monitors for the remote ses	sion		
	Use advanced location (winposstr)			
	Colors			
	Highest Quality (32 bits)	~		
	Display the connection bar when in full	screen mode		
	 Connection bar pinned (full screen) 			
	> LOCAL RESOURCES			~
			ADD CANCE	EL

RDP (Microsoft Remote Desktop) - Display

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: 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	t Remote Desktop)					×
GENERAL	✓ LOCAL RESOURCES					^
MORE	Pemote Computer Sound					
SECURITY	Keniote computer sound					
USER			Remote audio	recording		
FMAIL	Bring to this computer	~	Do not record		~	
NOTIFICATIONS	Keyboard					
ADVANCED	Reyboard					
	Apply Windows key combi example ALT+TAB)	inations (for				
	On the local computer	~				- 11
	Select the devices and the	e resources you v	vant to use in y	our remote session		
	Printers	Clipboard		Smart cards		
	Serial ports	Prompt fo	or selected reso	urces		
	✓ Hard drives	Other sup	ported Plug and	d Play (PnP) devices		
	> PROGRAMS					
	> EXPERIENCE					
	> CONNECTION					
						~
				ADD	CANCE	EL

RDP (Microsoft Remote Desktop) - Local Resources

Remote computer sound	Indicate what to do with the sound on the remote computer. Select between:
	Bring to this computer
	• Do not play
	Leave at remote computer
Remote audio recording	Indicate what to do with the audio recording on the remote computer. Select between:

	Do not recordRecord from this computer
Keyboard	Specify how key combination should be executed. Select between: • 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	Select the devices and resources that you wish to use on the remote computer. Select between: • 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 F	Remote Desktop)				×	
GENERAL	> GENERAL					^
MORE SECURITY	> DISPLAY					
USER INTERFACE	> LOCAL RESOURCES					
EMAIL NOTIFICATIONS	AIL OTIFICATIONS					
ADVANCED	Start this program on connection (altern	ate shell)				
	Program path and filename	Start in the fo	llowing folder			
	Use RemoteApp (seamless mode)					
	Program	Parameters				
	Execute the following program after log	'n	After login delay			
			500	* *		
	> EXPERIENCE					
	> CONNECTION					
	> ADVANCED					~
			ADD	CANC	EL	

RDP (Microsoft Remote Desktop) - Programs

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.

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)				×
GENERAL MORE SECURITY USER INTERFACE EMAIL	EXPERIENCE Performance Allow the following Choose the connection speed to optimize p	erformance		~
NOTIFICATIONS ADVANCED	 Default ✓ Desktop background Font smoothing Desktop composition ✓ Show window contents while dragging Menu and window animation ✓ Visual styles 	Redirect DirectX Redirect video playback redirect video playback redirect video playback	~	
	 Persistent bitmap caching Detect network automatically Reconnect if connection is dropped Load plug-ins in embedded mode Default Cache Default 	 Detect bandwith automatically Keep alive 0 	•	~
		ADD	CANCE	E

RDP (Microsoft Remote Desktop) - Experience

Choose the connection speed to optimize performance	Specify the connection speed to use to optimize the remote session performance. Select between:
	• Default
	• Modem (56 kbps)
	 Low-speed broadcast (256 kbps - 2 Mbps)
	 Satellite (2-16 Mbps with high latency)

	 High-speed broadcast (2-10 Mbps) WAN (>10 Mbps with high latency) LAN (> 10 Mbps with low latency)
Allow the following	Enable the following features on the remote computer: • 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 bandwith automatically • Reconnect if connection is dropped
Cache	Select the type of cache that will be used for the remote session:

	 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.
	i un 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	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 O Do not use RD Gateway server	 ✓ Initials 		~
	ADD	CANCI	EL	

RDP (Microsoft Remote Desktop) - Connection

Server authentication verifies that you are connecting to the intended remote computer.	If the actual verification does not meet minimum policy requirements, select what needs to be done by the remote computer between the following:
	 Connect and don't warn me
	Do not connect
	• Warn me

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:
	 Ask for password (NTLM)
	Smart card
	Smart cardAllow me to select later
	 Smart card Allow me to select later Use a gateway access token
Gateway access token	 Smart card Allow me to select later Use a gateway access token Provide the access token if the Logon method is set to Use a gateway access token.
Gateway access token Open gateway only when unable to ping host	 Smart card Allow me to select later Use a gateway access token Provide the access token if the Logon method is set to Use a gateway access token. Establish a connection with the RD Gateway server only when it is not possible to ping the remote computer.
Gateway access token Open gateway only when unable to ping host Bypass RD Gateway server for local addresses	 Smart card Allow me to select later Use a gateway access token Provide the access token if the Logon method is set to Use a gateway access token. Establish a connection with the RD Gateway server only when it is not possible to ping the remote computer. Bypass the RD Gateway server when connecting on a remote computer who has a local IP address.

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		×
U	se custom credentials		
	Username Domain		
	Store password on the local computer		
	Store password in the database		
	Password		
() Us	se credential repository		
	Select Credentials		
⊖ u	se my personal credentials		
о u	so privato vault soarch		
0.0			
	Search string		
		or	CANCEL
		UK	CANCEL

RDP (Microsoft Remote Desktop) - Gateway Credentials

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	 This will use the Windows Credential Manager. It is not the best option because it has the following limitations: 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, 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 <u>My Personal Credentials</u> .
Use Private Vault search	Use the Search string to search for credential entries in the Private Vault.

ADVANCED

RDP (Microsoft I	Remote Desktop)			×	
GENERAL	> CONNECTION				^
MORE	✓ ADVANCED				
SECURITY	Enable CredSSP support	Log off mode			
USER	Default V	Default	~		
EMAIL	Automatically logoff when disconnecting	Poconnoct modo			
NOTIFICATIONS	Default	Standard	~		
ADVANCED	DDD Version 7	Kente and levent			
	RDP version /	Reyboard layout	~		
		invariant cangaage (invariant country)			
	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 C	ANC	EL	

Microsoft Remote Desktop - (RDP) - Advanced

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: • Default
	Automatic
	RDM Agent

	Remote Desktop Services APIMacro
Automatically logoff when disconnecting	Automatically log off your RDP session when disconnecting.
Reconnect mode	Select the reconnect behavior. Select between: 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.
Restriced 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.

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)

Apple Remote [Desktop (ARD)		2	×
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Display Embedded (tabbed) V Credentials Default V Description	Monitor Primary monitor	~	^
	 LOGON SETTINGS Host Username Password ••••• 	Port 5900 Cefault port		
	 > SETTINGS > ADVANCED 			<
		ADD (ANCEL	

Apple Remote Desktop - General

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.

Password Analyzer	Indicates the strength of the password.

SETTINGS

Apple Remote [Desktop (ARD)		×	
GENERAL		.:		^
SECURITY	> LOGON SETTINGS			
USER INTERFACE	✓ SETTINGS			
EMAIL NOTIFICATIONS	Display			
ADVANCED	Scaled			
	Screen			
	Default 🗸			
	Miscellaneous			
	View only (input ignored)			
	Disable clipboard transfer			
	Authentication type			
	ARD	~		
	When viewing this computer and another login is using the display, what do you w to do?	ant		
	Connect to a virtual display	~		
	> ADVANCED			~
	ADD	CANCE	EL	
	Apple Remote Desktop - Settings			

Scaled	Scale the remote display to fit the window.

Screen	 Select the screen where you want to display the remote connection. Select between: 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)	Connect in view only mode. This option disables the keyboard and mouse while in session.
Request shared session	The remote user will be prompted with a request to share his session.
Disable clipboard transfer	Disable the clipboard sharing.
Authentication type	Select the authentication mode for the connection. Select between: • ARD • ARD ask observe • ARD ask control

ADVANCED

Apple Remote D	esktop (ARD)		×	
GENERAL	Description		1	^
MORE				
SECURITY				
USER	> LOGON SETTINGS			
EMAIL NOTIFICATIONS	> SETTINGS			
ADVANCED	✓ 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		L	

Apple Remote Desktop - Advanced

Mouse cursor	Select the way the mouse cursor is handled. Select between:
	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.

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: • On the local computer • On the remote computer • In full screen mode only
Keyboard layout	Select the keyboard layout. Select between: • Azerty • Qwerty
Preferred encoding	 Change the encoding to use less bandwidth. From the least to the most bandwidth used, select between: 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	2	×
GENERAL MORE SECURITY USER INTERFACE	Name • The name is required. Folder Vault (Windjammer IT)	Image	^
EMAIL NOTIFICATIONS ADVANCED	Display Monitor Embedded (tabbed) Primary monitor Description Alarm Codes 		
	Name Employee Code Alarm Code No data to display	ADD CANCEL	v

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 ••••• Employee code 1234 Note	☑ Is hidden		
Alarm code for May 2018		ок	CANCEL

New Alarm Code

Employee		Enter the employee's name.
Alarm code	4	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

 \times

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**.

Information -	Email Account		🛛 🗙
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Display Embedded (tabbed) Cescription GENERAL POP3 IMAP SMTP	Monitor Primary monitor	Image
		AD	D CANCEL

Information Entry - Email Account - General Tab
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 - I	Email Account		2 ×
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Display Embedded (tabbed)	Monitor Primary monitor	*
	Host Name Username SSL 3.0 Authentication Password	Port 110 Password	•
	 IMAP SMTP 	ADD	CANCEL

Information Entry - Email Account - POP3 Tab

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.
Authenticati on	Choose your POP3 authentication mode between: AppleToken
	HTTPMD5Digest
	MD5ChallengeResponse
	• NTLM
	Password

IMAP

Information -	Email Account		× 12
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Display Embedded (tabbed) Description GENERAL POP3 IMAP Host Name Username SSL 3.0 Authentication Password	Monitor Primary monitor Port 143 Password	
	► SMTP	Δ	DD CANCEI

Information - Email Account - IMAP Tab

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.

Authenticati on	Choose your IMAP authentication mode between: AppleToken
	HTTPMD5Digest
	MD5ChallengeResponse
	• NTLM
	Password

SMTP

Information -	Email Account		2 ×
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Email Account Description GENERAL POP3 IMAP SMTP Host Name My outgoing server (3 Use same settings as Username SSL 3.0	SMTP) requires authentication my incoming mail server Password	Port 25
	Authentication Password		Ψ

ADD CANCEL

Information Entry - Email Account - SMTP Tab

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 server	Use POP3 or IMAP settings for the outgoing server authentication.
Username	Enter the SMTP username.
Password	Enter the SMTP password.
SSL 3.0	Enable if the SMTP requires an SSL connection.
Authentication	Choose your SMTP authentication mode between:
	• 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.

Information -	Website	2	×	
GENERAL MORE SECURITY USER	Description	.:		^
INTERFACE EMAIL NOTIFICATIONS ADVANCED	Website Enable web browser extension link			
	Add Equivalent URL CREDENTIALS Credentials Default	~		
	Username Domain			
	Password •••••• > CUSTOM FIELDS	:		*
	ADD	CANCI	EL	

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

Information Entry - Website

Website	Enter the URL to a website's log in page.
Credentials	 Select the credential mode between: Default: provide the credentials in the entry's properties.

		 Credential repository: select an existing credential entry. 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.

Information	- Secure Note	2 ×
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Display	Image
	Embedded (tabbed) Description Secure Note	Primary monitor
	□ Is sensitive Heading 1 ▼ B Image: Second control of the second control o	HTML
		ADD CANCEL

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 Entry - Note/Secure Note

5.3.2.3 Contact

DESCRIPTION

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

GENERAL

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

Contact - Cus	stomer	⊠ ⊗
	General	
GENERAL	First name	Image
MORE	×	
DETAILS	· · · · · · · · · · · · · · · · · · ·	
SECURITY	Gender	
USER INTERFACE	Unspecified \lor	
ADVANCED	Middle name	
	7	
	Prefix	
	Last name	
	F	
	Job title	
	7	
	Customer #	
	×	
	Folder	
	GroupFolder	
		•••
	Type	
	Customer	~
	Display	
	- · · · · · · ·	
		ADD CANCEL

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 - Cus	stomer			×	⊗
GENERAL MORE DETAILS SECURITY USER INTERFACE ADVANCED	Address Company City City City Famail/Phones Email Work phone Fax Vebsite	Address			* × ×
			ADD	CANC	EL

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 New Entry		2 ×
 Entry Session Information Contact Document Folder Credential Entry Template Import 	<search> Image: Certificate Image: Document Image: Document<th> Data Source Configuration (.rdd) Email Image Microsoft OneNote Microsoft Visio PDF Text (RTF) </th></search>	 Data Source Configuration (.rdd) Email Image Microsoft OneNote Microsoft Visio PDF Text (RTF)
		CONTINUE CANCEL

Add a new Document Entry

Document		🛛 🗶
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Description Document Mode Stored in database	Image
	AD	D CANCEL

Document Entry - Default

File Type	Indicate the file type entry you wish to create.
Mode	Select the mode between: • Stored in database (select a file stored in the database) • URL (open a file using a URL)

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.



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.

Add New Entry		2 ×
 Entry Session Information Contact Document Folder Credential Entry Template Import 	Search> Company Database Domain Identity Server Software	 Customer Device (router, switch, firewall,) Folder Printer Site Site Workstation
		CONTINUE CANCEL

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.

Folder - Fold	er 🔀 😣
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Image GroupFolder Image Devolutions Web Login Image Credentials Image Default Image Default Image Default Image Default Image Default Image Image Image Image Image Devolutions Web Login Image Image <t< td=""></t<>
	ADD CANCEL

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.

Private Vault Devolutions Web Login Devolutions Personal devolutions_Personal Children entries	FL wind Information	- Login (Web)	⊠ ⊗
 vvind Personal Info Home Alarm National Bank Visa 	GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name vwind GroupFolder Devolutions Web Login Display External V Primary monitor	Image E
		Description Website http://windsrv	<u>/</u>
Inherited Credentials set or children entry	n the	Credentials Credentials Inherited	~
		UPDA	TE CANCEL

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.

Credentials -	Connection String	2 ×
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Cescription GENERAL Data source Microsoft SQL Server Data provider .NET Framework Data Provider for SQL Server Connection string	Image
	A	DD CANCEL

Credentials - Connection String

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 Passw ord (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
	AE	D CANCEL

Credentials - One-Time Password

Кеу	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: • 6 Digits
	• 8 Digits
Hash algorithm	Select the secure hash algorithm used to generate the verification code. Select between:
	• 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

5

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

Credentials - I	Password List			🛛 🗙
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Description Password List User	Description No data to display		hage
			ADD	CANCEL

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	y.
---	----

Password		×
Host		
User		
Domain		
Password	0	:
Description		•
Expires after		_//
Sort priority		
0	OK CANCEL	

Password List - Password

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

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.

Credentials - F	Private Key	🛛 🗶
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault GENERAL ADVANCED Private key type Data Passphrase Passphrase Prompt for passph	Image
	Password •••••• Private Key Data	:
	A	DD CANCEL

Private Key Entry - Properties

Private Key Type	 Select between: 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.

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.
٩	Click to download the private key as a .ppk file.
GENERAL	ADVANCED
Automatically loa	d to key agent

Private Key Entry - Properties - Advanced

Automatically load to key agent	Automatically load the Private Key in the <u>Key Agent Manager</u> 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.

Credentials - U	Jsername / Password	2	×
GENERAL MORE SECURITY USER INTERFACE ADVANCED	Name Folder Private Vault Description GENERAL Username Domain Always ask password Password Mnemonic password	Image	
	Al	DD CANCE	

Username / Password - Properties

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

Password	Enter the password. Click I to reveal the password. Click the advanced button I to generate a password or open the Password generator for more settings and password choices.
Mnemonic password	Enter a phrase to help remember the password.

5.3.2.7 Import

DESCRIPTION

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

Add New Entry		🛛 🗙
 Entry Session Information Contact Document Folder Credential Entry Template Import 	Search> Import (.rdm, .pvm, .xml) KeePass (.xml)	
	CONTINUE C	ANCEL

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				×
 Entry Session Information Contact Document Folder Credential Entry Template Import 	<search> Import (.rdm, .pvm, .xml)</search>	KeePass (.xml)		
		CONTINUE	CANCE	L

Add New Entry - Import

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

Import Entries				× ×
	2	3		
File Selection	Analyze	Import		
Select a File				
Entries.rdm	•••			
Import in folder				
Vault (Service Desk)	•••			
Master key				
			BACK	NEXT 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**.

Import Entries	Folder	52 (8)	8 8
File Selection	<u> </u>		
Select a File Entries.rdm Import in folder Vault (Service Desk) Master key •••••	 Vault (Service Desk) Non-Production General Orion.loc Production Confidential General TestFolder 		
		OK CANCEL	BACK NEXT CANCEL

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			× ×
	2	3	
File Selection	Analyze	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				∞ ⊗
Tile Selection	n Analyze	Import		
Add V A	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	2345 > »		98 Results
			BACK NEXT	CANCEL

Import Entries - Analyze

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

Import Entries			× ×	
Tile Selection	2 Analyze		•	^
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

Pevolutions Password Server	MPV My Private Vault 🗸 🗸 🗸 🗸 🗸 🖌 🗸	🖂 🛑
Dashboard	REPORTS	
Vaults	Login	
💮 My Private Vault		
Search		
Favorites	Connected Login Attempt Login History User List	
Reports	Entries	
Administration		
	Opened Expired Entry Password Connections List Analyzer	
	Logs	
	Activity Logs Data Source Administration Deleted Logs Logs Entries	
	Configuration	
	越 🖬	
	Scheduling Diagnostic Reports	
2019.1.20.0		

Reports

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

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 Password Server data source.
Administration Logs	This displays the Admin logs of the Devolutions Password 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.

E Productions	My Private Vault 🗸 🖌						
Dashboard	REPORTS > LOGIN HISTORY						
Vaults	(count choose a						
R. My Private Vault	V Username @	Creation Date	Last update date	Token expiration date	♥ Source	∇ Platform	
Q. Search	david@windjammer.loc	10/29/2019 09:35	10/29/2019 09:35	10/29/2019 11:04	Web	Web	
- search	DH david@windjammer.loc	10/29/2019 09:20	10/29/2019 09:20	10/29/2019 11:04	Web	Web	
14 Favorites	avid@windjammer.loc	10/28/2019 13:51	10/28/2019 13:51	10/29/2019 11:04	Web	Web	
🕻 Reports	DH david@windjammer.loc	10/28/2019 13:21	10/28/2019 13:21	10/29/2019 11:04	Web	Web	
Administration	(avid@windjammer.loc	10/24/2019 13:57	10/24/2019 13:57	10/29/2019 11:04	Web	Web	
	DH david@windjammer.loc	10/24/2019 12:53	10/24/2019 12:53	10/29/2019 11:04	Web	Web	
	(avid@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	
	(avid@windjammer.loc	10/23/2019 15:17	10/23/2019 15:17	10/29/2019 11:04	Web	Web	
	(avid@windjammer.loc	10/22/2019 14:44	10/22/2019 14:44	10/29/2019 11:04	Web	Web	
	Export		x < 1 > x			10 Results	

Filtering and Sorting Reports

COLUMN CHOOSER

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

REPORTS > LOGIN HISTORY					
Column Chooser =					
 Last update date Token expiration date 					
 Source Platform 	ner.loc				
DH david@windjammer.loc					

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.



Reports - Scheduling Reports

To create a new Scheduling Report, click on the Add button.
Event		2 ×
General Expired Entry List Recipients _administrator Title My Expired Entry List Start 09/03/2019	✓✓	Filter ✓ Include expired ✓ Include manually flagged expired Expiring in 7 ▲ day(s)
 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

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.

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

Filter options

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

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 Password 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 Password Server content.

Pevolutions Password Server		🛛 Default 🗸		
(2) Dashboard	REPORTS > DIAGNO	STIC		Ē,
🛞 Vaults	DATA SOURCE	DATA SOURCE		^
📳 My Private Vault		SERVER NAME	DPS	
O Search		SERVER DESCRIPTION		
		SERVER VERSION	2019.1.20.0	
Favorites		DB VERSION	523	
🖺 Reports		CURRENT REPOSITORY ID	0000000-0000-0000-0000-0000000000000000	
		CURRENT REPOSITORY NAME	Default	
		ENTRIES SIZE	445.9 kB	
		SETTINGS SIZE	1.5 kB	
		USER SPECIFIC SETTINGS SIZE	0.1 kB	
		CONNECTION PROTOCOL	http	
		ALLOW CONNECTION STATES	Yes	
		DATA		
		REPOSITORY COUNT	6	
		ENTRY/ITEM COUNT	254/248	
		SESSION COUNT	93	
		DATA ENTRY COUNT	27	
		CREDENTIAL COUNT	20	
		SUB CONNECTION COUNT	0	
		DOCUMENT COUNT	2	
		CONTACT COUNT	3	
		SUB TOTAL	145	
		SESSION TOOL COUNT	4	
		GROUP COUNT	99	
		TOTAL COUNT	248	
		VIRTUAL FOLDER COUNT	0	
		CUSTOM IMAGE COUNT	1	
		RTF NOTE COUNT	0	
		VERSION		
		CONNECTION HISTORY VERSION	0x000000000005EBC	
		CONNECTION SERVER VERSION	0x000000000005E93	
2019.1.20.0				*

Reports - Diagnostic

5.5 Administration

DESCRIPTION

The **Administration** section is <u>only available for administrators</u>. 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

ADMIN	IISTRATION > USEF	s							+	5	\$	>
	Username 🗢	Full name 🗢	Authentication Type	User Type	is enabled	Reset 2FA requested	Last Login	Last Login				
VH	victor@windja	Victor Hedm	Domain	User	~	×			5	6	1	D
SA	sa		Database	Administrator	\checkmark	×			6	a ,	1	D
BP	bill@windjamr	Bill Preston	Domain	User	~	×	1/28/2019 1	a day ago	6	θ,	1	Ì
ER	ellen@windjar	Ellen Ross	Domain	User	~	×	1/29/2019 1	3 hours ago	6	θ,	1	D
JS	jeff@windjam	Jeff Smith	Domain	User	~	×	8/3/2018 11:	6 months ago	6	۵,	1	Ì
AB	allan@windjar	Allan Brewer	Domain	User	~	×	7/25/2018 0	6 months ago	6	θ,	1	D
BG	burton.guido@	Burton Guido	Domain	User	~	×			6	۵,	1	D.
DH	david@windja	David1 Hervi	Domain	Administrator	~	×	1/29/2019 1	an hour ago	6	a ,	1	1

Administration - Users

GLOBAL OPTIONS

+	Add a user.
â	Import users from LDAP.
C	Refresh users list.

USER OPTIONS

FG	See user activity report.
	Change password.
/	Edit user settings.
Ē	Delete user.

5.5.1.1.1 General

DESCRIPTION

Edit user				2 × 12
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	GENERAL Authentication type Office 365/Azure AD User • ellen@downhillpro.xyz User type User Must change passwoo INFORMATION	∽ rd at next logon	User license type Default	✓ ✓ ✓ Enabled
	Ellen Email • ellen@windjammer.loc		Ross	
				UPDATE CANCEL

Edit Users - General

Authentication type	 Select the user's authentication type: Custom (Devolutions): create a user in Devolutions Password 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)	Enter the user login name.
User type	 Choose the user type: 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	 Select the type of the license that the user has: Default: Connection Mangement. Connection Management: for users who open remote connections. Password Management: for users who only use Devolutions Password Server as a password manager.
Enabled	Check to activate the user.
Must change password at next	Check to force the user to change the password next time they log on.

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

The	Information	section i	s for i	ontional	information
	mormation	Secuoni	5 101 1	opuonai	mornauon.

Edit user		2 ×
GENERAL	INFORMATION	
INFORMATION	Company	Job title
TWO FACTOR	*	
ROLES	Department	Gravatar email
APPLICATIONS		ellen@windjammer.loc
VAULTS		
SETTINGS	ADDRESS	
EMAIL NOTIFICATIONS	Address	State
	Country	
	Select Country 🗸	
	PHONE	
	Phone	Work
	Mobile	Fax
		UPDATE CANCEL

Edit User - Information

5.5.1.1.3 Tw o Factor

DESCRIPTION

If you set two-factor authentication as <u>optional per user in Password Server Settings</u>, you then need to configure which 2FA method to use.

SETTINGS

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

Edit user			×
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS PRIVILEGES PERMISSIONS REPOSITORIES SETTINGS EMAIL NOTIFICATIONS	Type None (current) Google Authenticator Yubikey Email		
	UPDATE	CANC	EL

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 - Two Factor

5.5.1.1.4 Roles

DESCRIPTION

Assign users to a **Role**.

Edit user						×
GENERAL	i Only custom roles o	an be manually assigned.				
TWO FACTOR	🗙 Unselect All 🗸 Sel	lect All				
APPLICATIONS	Name 📤	Description	Role Type 🗢	Is member		
VAULTS	WINDJAMMER\Vault	Password Vault Users	Active Directory			
SETTINGS EMAIL NOTIFICATIONS	WINDJAMMER\Vault		Active Directory			
	WINDJAMMER\RDM	Service Desk Staff - I	Active Directory			
	Show-IT Corp	Azure/Office365	Office365	~		
	WINDJAMMER\Vault	Groups from IT Depa	Active Directory			
	Show-Corporate	Azure/Office365	Office365	\checkmark		
	WINDJAMMER\RDM	Full administrators	Active Directory			
	WINDJAMMER\Vault	CAL Non-IT Users	Active Directory			
	WINDJAMMER\HR		Active Directory			
	WINDJAMMER\Servic		Active Directory			~
				UPDATE	CANC	EL

Edit User - Roles

Roles	Check the Is Member box to assign the role to the user. Consult <u>Role Management</u> 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

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

5.5.1.1.6 Vaults

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

For more information, please consult the <u>vaults</u> topic.

Edit user			🛛 🗙
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	NameDownhill ProTelemarkWindjammer CorpWindjammer DefaultWindjammer ITWindjammer IT Vault	Description Customer since 2015 Customer since 2017 Password Vault for non-administrative per Default Repository - Shortcuts and commo For the IT departement exclusive use For IT personnel without the need for Con Image:	Allow
		UPDATE	CANCEL

Edit User - Vaults

5.5.1.1.7 Settings

Edit user			🛛 🗙	
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	Offline mode Read-only		~	
		UPDATE	CANCEL	



Allow the user to enable <u>Offline Mode</u> on the data source. The data source also needs to be configured to permit offline mode. There are 4 modes available:

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 <u>Advanced Data Sources</u> only.
Read/Write	An advanced cache, with change synchronization. This mode is allowed for <u>Advanced Data Sources</u> only.

5.5.1.1.8 Email Notifications

DESCRIPTION

Email Notifications are real-time alerts that are sent to specific users. The notifications are sent when certain items in Devolutions Password Server are added, modified or deleted.

SENERAL	- EMAIL NOTIFICATIONS				
TWO FACTOR	Item 🕇	Enabled	Added	Edited	Deleted
ROLES	Connection opened	~			
APPLICATIONS	Data Source Settings changed				
PERMISSIONS	Entries	~			~
REPOSITORIES	Repository	~			
MAIL NOTIFICATIONS	Roles	~	~	~	~
	Security groups				
	Tasks				
					~
	Users				
	Users locked out - WATCHED BY V Username		Active	On Edit	On Delete
	Users Users locked out + - WATCHED BY VIsername - admin	 ✓ < 1 → κ is 	Active	On Edit	On Delete
	Users Users locked out	 ↓ ↓	Active	On Edit	On Delete
	Users Users locked out	 ▼ < 1 → × Is 	Active	On Edit	On Delete
	Users Users locked out	 I I	Active	On Edit	On Delete
	Users Users locked out	✓ 1 → x	Active	On Edit	On Delete
	Users Users locked out		Active	On Edit	On Delete
	Users Users locked out		Active	On Edit	On Delete
	Users Users Userslocked out		Active	On Edit	On Delete
	Users Users Userslocked out		Active	On Edit	On Delete
	Users Users Users Users Users * * * * * * * * * * * * *		Active	On Edit	On Delete

Edit Users - Email Notifications

Connection opened	Sends notification when a connection is opened.
System Settings	Sends notification about modifications in the <u>System</u> <u>Settings</u> .
Entries	Sends notification about modifications to entries. It could be set for Add, Edit and/or Delete.
Vaults	Sends notification about modifications to Vaults. It could be set for Add, Edit and/or Delete.
Roles	Sends notification about modifications to <u>Roles</u> . It could be set for Add, Edit and/or Delete.

Tasks	Sends notification about modifications to Tasks. It could be set for Add, Edit and/or Delete.
Users	Sends notification about modification to users. It could be set for Add, Edit and/or Delete.
Users Locked Out	Sends notification when a user is locked out after multiple failed login attempts.

5.5.1.2 Applications

DESCRIPTION

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

ADMINISTRATION > APPLICATIONS				+ C	
Name 🔶	App Id 🗢	Is enabled	Last Login	Last Login	
		No dat.	a to display		

Administration - Applications

Application		2	×
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 • KaGS6wv1Ph0OmIGEXZVWueyYh65e4Rtjh6e5W2uZsjcPaTQoj94b96VKxtFmHl82 Fnabled		
	Add	Can	cel

Administration - Applications - New Application

Name	Display name of the Application key.
Application key	Application key to be use in the application to communicate with Devolutions Password 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

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

Password Server	😡 Windjammer IT 🗸 🗸			\boxtimes	DH
Administration > Vaults			-	F	0
🕅 Name 🔺	♥ Description ♦				
Downhill Pro	Customer since 2015		ê	00	
Telemark	Customer since 2017		•	10	
Windjammer Corp	Password Vault for non-administrative personnel		4	80	Î
Windjammer Default	Default Repository - Shortcuts and common tools	/	4	80	
Windjammer IT	For the IT departement exclusive use		ê	10	
Windjammer IT Vault	For IT personnel without the need for Connection Management	/	ê	10	
III Export	н ∢ 1 → н			6 Re	sults

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*.

ADMI	NISTRATION > USERS LOCKED		0
	Name 🔺		
E	Ellen		£
		N ≪ 1 → N	1 Results

Administration - Users Locked

ADMINISTRATIC	DN > USERS LOCKED	Ø
Name 🔺		
EL Ellen		6
_	H 1 ▶ H	1 Results
U	Jnlock 🗙	
	Do you really want to unlock the selected user(s)?	
	YES NO	

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

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



The <u>Email</u> and the <u>Scheduler</u> 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 <u>Subscriber</u> and a <u>Subscription</u> need to be created. It is also possible to regroup Subscriber in <u>Subscriber Groups</u> to send notifications to a group of subscribers.

5.5.1.7.1 Subscribers

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

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

≡	Devolutions Password Server		DP Downhill Pro 🗸		⊠ _
O,	Administration > No	TIFICATIONS > SUBSCRIBE	RS		+ 😋
ß	Name 🔺	Type 🗢	Groups 🗢	Subscriptions \$	Add
☆	Bob Anderson	Email	0	0	/ 💼
۲					
•			N 4 1 > H		1 Results

Create a Subscriber

Fill in the information in the following fields.

Subscriber	🛛 🗙
Name •	
Bob Anderson	
Туре •	
Email	~
EMAIL Email Address: •	
bob@windjammer.co	
Recipient Name:	
Bob Anderson	
Save	Cancel

Email Subscriber properties

Subscriber	2 ×
Name •	
Syslog Server	
Type •	
Syslog	~
LOG TO SYSLOG SERVER	
Use default 🚯	
syslog.windjammer.loc	
Port: •	
9997	▲ ▼
Protocol: •	
ТСР	~
	Save Cancel

Syslog Server Subscriber properties

Name	Display name in the Subscribers list.
Туре	 Email : The notification will be sent to an email address.
	o Email Address: Valid email address.
	\circ Recipient name: Email recipient name.
	• Syslog : The notification will be sent to a syslog server.

 Use default: Will use the Syslog server configuration set in <u>Logging</u>.
$_{\odot}$ 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

TBD

5.5.1.7.3 Subscriptions

DESCRIPTION

TBD

- 5.5.2 Configuration
- 5.5.2.1 System Settings

DESCRIPTION

The System Settings allow the administrators control many global aspects of the Devolutions Password Server data source. Manage settings such Offline Mode, password policies, version management, etc.

≡	Devolutions Password Server	MPV My Private Vault 🗸 🗸 🗸 🗸 🗸 🖌 🗸	M 🛑
Θ	ADMINISTRATION > DATA SO	URCE SETTINGS	8
	GENERAL SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY USER TEMPLATE EMAIL NOTIFICATIONS	GENERAL Allow user specific settings Automatic check in after Automatic check in after Default	
2019.1.20.0	ADVANCED	COMMENTS Allow log comments editing Minimum length (char) 0 FILE SIZE	

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.

≡	Devolutions Password Server		🥨 Windjammer IT 🛛 🗸	
Ø	Administration > system	SETTINGS		
8	GENERAL	GENERAL		
¶ 0 ਨ	SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY	 ✓ Allow user specific settings △ Automatic check in after Add entry mode Default 	 Allow entry states (Lock, Running, Checkout) 60 minutes 	
Ē.	USER TEMPLATE EMAIL NOTIFICATIONS ADVANCED	COMMENTS Allow log comments editing Minimum length (char) 0 FILE SIZE Maximum file size (MB) 25	▲ ▼ ■	

Administration - System Settings - General

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: • Default • Template list (include blank) • Template list only • No template selection

Allow log comments editing	Enable the log comment editing for all users.
Minimum length (char)	Minimum length in character for the comment.
Maximum file size (MB)	Limit the size of attachments and document entries to avoid to over load the data source.

Allow favorites	Allows to flag entries as favorites.
Allow Private Vault	Allow users to use the Private Vault.
Log Private Vault activities	Include the logs of the <u>Private Vault</u> for all users of the data source.
Allow credential repository in private Vault	Allow credential repository for sessions in the <u>Private</u> <u>Vault</u> .

Use legacy security	Enable the legacy security
Time Zone	Select the time zone you are currently in.
Days	 Select which days the session is available for. Select between: 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	 Select the hours which the session is limited to. Select between: 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 Password Server data source no matter which method will be used (web interface, Remote Desktop Manager).

Devolutions Password Server	Win	ndjammer IT 🛛 👻	🖂 머
Administration > system	SETTINGS		8
GENERAL SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY USER TEMPLATE EMAIL NOTIFICATIONS ADVANCED	SYSTEM MESSAGE	hanged	i.

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.

=	Devolutions Password Server		🥘 Windjammer IT	~
ø	ADMINISTRATION > SYSTEM SETTINGS			
€ € € €	Image: Second state sta	PASSWORD Password history 5 Password strength calculator Default		美
		Pwned check ♥ None ADVANCED Disable password saving (shared) Disable password saving (user specific settings) Allow reveal credentials (if enabled in the entry) Allow password in macro (send keys)	Disable password savi	v ng (tools) able for all sessions

Administration - System Settings - Password Policy

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.
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 enabled in the entry)	Shows the credentials if the box "Allow show credentials (everybody)" is check inside 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 Passw ord Template

DESCRIPTION

≡	Devolutions Password Server	😡 Windjammer IT 🗸 🗸
ß	ADMINISTRATION > SYSTEM SETTINGS	
۲	GENERAL	PASSWORD TEMPLATE
8	SYSTEM MESSAGE	Default template
•	PASSWORD POLICY	Strong Policy 🗸
O,	PASSWORD TEMPLATE	✓ Force default template
☆	FORBIDDEN PASSWORD TYPE AVAILABILITY	PASSWORD VALIDATION
		Password Validation
Ē	EMAIL NOTIFICATIONS	None 🗸
毘	ADVANCED	

Administration - System Settings - Password Template

SETTINGS

Password Validation	Select a password template to use. Consult the <u>Password</u> <u>Template</u> page for more information.
Force default template	Enforce the default template.
Password Template	 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 Passw ord

DESCRIPTION

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

=	Devolutions Password Server		\boxtimes	DH
0	ADMINISTRATION > SYSTEM SETTINGS			8
8	GENERAL	FORBIDDEN PASSWORD		
10	SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY	Case sensitive Veri	fication Mode	:
্ ্ রু		123456,password,qwerty,654321, <u>pwd</u>		
۵ بی	USER TEMPLATE EMAIL NOTIFICATIONS ADVANCED			
		+ Import	业 Export]

Administration - System Settings - Forbidden Password

Case sensitive	Make the verification mode case sensitive.
Verification mode	Select the verification mode between:

	Contains : the password will be forbidden if it contains a word in the blacklist.
	Exact match : the password will be forbidden if it matches a word in the blacklist.
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 Password Server data source. Each section contains different entry types you can choose to be available.
	Devolutions Password Server	
@	Administration > systems	SETTINGS
 	GENERAL SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY USER TEMPLATE EMAIL NOTIFICATIONS ADVANCED	 TYPE AVAILABILITY + Expand all - Collapse all > • Session > • E Information > • E Contact > • E Document > • E Folder > • Credential Entry

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.

≡	Devolutions Password Server	😡 Windjammer IT	~
ß	Administration > systems	SETTINGS	
8	GENERAL	USER TEMPLATE	
1 0	SYSTEM MESSAGE	Offline mode	
০ 、 শ্ব	PASSWORD POLICY PASSWORD TEMPLATE FORBIDDEN PASSWORD TYPE AVAILABILITY	Read-only User User	~
E R	USER TEMPLATE EMAIL NOTIFICATIONS ADVANCED	Default	~

System Settings - User Template

Offline mode	This option will only affect Remote Desktop Manager application.
	The possible values are : • Disabled • Read only • Read/write
User type	The possible values are : • Administrator • User • Read only user
User license type	Select if users are prompted to choose a template when creating a new entry. Select between: • Default • Connection Management • Password Management

DESCRIPTION

≡	Devolutions Password Server	🧓 Windjammer IT 🛛 👻			🖂 🖸
Ø	ADMINISTRATION > SYSTEM SI	ETTINGS			Ë
) • •	GENERAL SYSTEM MESSAGE PASSWORD POLICY PASSWORD TEMPLATE EORPIDDEN BASSWORD	Username _admin allan@windjammer.xyz	Enabled	On Edit	On Delete
☆	TYPE AVAILABILITY USER TEMPLATE	bill@windjammer.loc			
R	ADVANCED	david@windjammer.loc ellen@downhillpro.xyz			
		ellen@windjammer.loc jeff@windjammer.loc			
		sa Ted@downhilipro.xyz			
		ted@windjammer.loc Victor@windjammer.xyz			
		william@windjammer.xyz ⊮ ≪ 1 → H			

Administration - System Settings - Email Notifications

5.5.2.1.9 Advanced

DESCRIPTION

≡	Devolutions Password Server	
ß	ADMINISTRATION > SYSTEM S	SETTINGS
	GENERAL	ADVANCED
	SYSTEM MESSAGE	Disable stack trace
0	PASSWORD POLICY	
U,	PASSWORD TEMPLATE	
∽	FORBIDDEN PASSWORD	
~	TYPE AVAILABILITY	
199	USER TEMPLATE	
E	EMAIL NOTIFICATIONS	
愚	ADVANCED	

Administration - System Settings - Advanced

5.5.2.2 Password Server Settings

DESCRIPTION

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

DMINISTRATION > PASSWORD	SERVER SETTINGS > GENERAL	=
SENERAL		
Name		
Devolutions Password Server		
Description		
Devolutions inc.		
DNS Name		
Server		
SERIAL Server User limit: Unlimited users		
SERIAL Server User limit: Unlimited users Edition: Platinum		
SERIAL Server User limit: Unlimited users Edition: Platinum Expiration:		
SERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL		
SERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL		
SERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL User limit: 1 users		
SERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL User limit: 1 users Launcher CAL		

Administration - Password Server Settings - General

GENERAL

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

DNS Name	Name of the DNS server.

SERIAL

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

	Pevolutions Password Server
B	ADMINISTRATION > PASSWORD SERVER SETTINGS > AUTHENTICATION
⊗	AUTHENTICATION MODES
(3)	 Authenticate with domain user Authenticate with Office365 user
0	✓ Authenticate with Devolutions Password Server custom user
~	WINDOWS AUTHENTICATION
~	Enable Windows authentication
1	Configuration
限	
	Domain Office365

Adminsitration - Password Server Settings - Authentication

AUTHENTICATION MODES

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 Password Server custom user	The Devolutions Password Server is used to authenticate the user. You must create the initial user through the console.

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

CONFIGURATION

Domain	Configure the <u>Domain</u> type.
Office365	Configure the <u>Office365</u> type.

DESCRIPTION

The domain is used to authenticate the user. <u>This is the most secure, flexible and</u> <u>easiest to manage</u>. No need to sync users between the domain and Devolutions Password Server. On first use of the Devolutions Password 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 Password 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.

OMAIN AUTHENTICATION		
Domain		
windjammer.loc	*	
Container		
CN=Users,DC=windjammer,DC=loc		
Administration credentials		
administrator	Change	
Allow logins using email address		
DAPS		
Enable LDAPS		
Port		
Default		
Custom		
1ULTI DOMAIN (DISABLED)		
Multi domain		
Trusted domains		
	Change	
UTOMATIC USER CREATION		
Auto create domain users in database		
Create read-only user		
Default Vault		
None	~	
Only from this AD group		
	Change	
Username Format		
UPN	\checkmark	
OMAIN USERS AND ROLES CACHE		
Enable domain cache feature		
Update users and groups data every:		
A 11		
30 Minutes		

Authentication - Configure Domain

DOMAIN AUTHENTICATION

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 Password Server instance. The email address field must be filled in the User Management.

LDAPS

Enable LDAPS	Enable the LDAP over SSL communication.

Port	Default: LDAPS default communication port.
	Custom : Set a specific port value.

MULTI DOMAIN (DISABLED)



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

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

AUTOMATIC USER CREATION

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.

Username Format	Select the username format that will be created in the database.
	 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

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 Password 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 <u>Azure portal configuration guide for Office 365 authentication</u>.

The **Office365** tab allows Devolutions Password Server to authenticate users using **Office365** authentication. <u>All fields are mandatory</u>.

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-c000-00000000000	
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	\sim
OFFICE365 USERS AND ROLES CACHE	
Undate upon and groups date evens	
0 Hours 30	
Test Connection	

Authentication - Configure Office365

OFFICE365 PARAMETERS

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

NATIVE APPLICATION (RDM)

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

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

USERS AND ROLES CACHE

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

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

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.

ENERAL	
Name	
Devolutions Password Server	
Description	
Devolutions inc.	
DNS Name	
ERIAL Server	
ERIAL Server User limit: Unlimited users	
ERIAL Server User limit: Unlimited users Edition: Platinum	
ERIAL Server User limit: Unlimited users Edition: Platinum Expiration:	
ERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL	
ERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL	
ERIAL Server User limit: Unlimited users Edition: Platinum Expiration: User CAL User limit: 1 users	

Administration - Password Server Settings - Email

GENERAL

Email enabled	Enable the Email feature.

SMTP CONFIGURATION

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 <u>Note 1</u> 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 Password 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. <u>This alternate connection method using SSL is not currently supported</u>.

5.5.2.2.1.4 Logging

DESCRIPTION

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

ADMINISTRATION > PASSWORD SERVER SET	TINGS > LOGGING	
GENERAL		
Log debug information		
Language		
English	•	
Scheduler log path		
SYSLOG SERVER		
Log to Syslog server		
Host		
Port		
	V	
Protocol		
ТСР	•	
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

Log debug information	Enable the Devolutions Password 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

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: • TCP
	• UDP

WINDOWS EVENT LOG

Event Log	Send the logs to Windows Event Log.

SLACK INTEGRATION

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 section allows the administrator to configure the web interface features.



Administration - Password Server Settings - Features

SETTINGS

Allow browser extensions Devolutions Web Login)	Allow to save credentials in the Devolutions Password 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 Password Server. Some further configurations are needed to be done before enabling these options.

The <u>Email</u> settings must be configured in the Devolutions Password Server instance in order for notifications to be sent.

DMINISTRATION > PASSWORD SERVER SETTINGS > SCHEDULER		
IOTIFICATION		
Allow notification subscription		
Time Zone		
(LITC-05:00) Eastern Time (LIS & Canada)	v	

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.

Allow notification subscription	Enable the notifications of the Devolutions Password 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.

MINISTRATION > PASSWORD SERVER SETTINGS > ADVANCED		
DVANCED		
Token Valid Time (minutes)		
1440	▲ ▼	
Inactivity time (minutes)		
240	▲	
User license type		
Default	•	
Launch connection with		
Default	•	
Client HttpRequest cache coun	t.	
20		

Administration - Password Server Settings - Advanced

SETTINGS

FEATURES

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 Password Server instance. The maximal value is 1440 minutes which is 24 hours.	
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 Tw o-Factor

DESCRIPTION



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

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

Devolutions Password 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	2FA is enforced on an individual basis. The administrator chooses who uses 2FA and what product or technology they use.
	Choose this option if not all users are set up for two- factor authentication.
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 Password Server **administrators** or a **specific email**.
- If you chose to send reset requests to an email address instead of the Devolutions Password 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
Optional per user - 2
Send reset email to
Administrator(s) - 3
Specific email
4
SUPPORTED 2FA 😮
Google 5
✓ Yubikey
🖌 Email 🌣 Configure
SMS
Duo
SafeNet
AuthAnvil
Radius
Vasco
DEFAULT
Default
Google Authenticator
ALTERNATE
✓ Email 7
Backup codes

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 <u>Edit Users</u> for more information.

Edit user		5	3 ×
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS PRIVILEGES PERMISSIONS REPOSITORIES SETTINGS EMAIL NOTIFICATIONS	Type None (current) Google Authenticator Email SMS		
	UPD	DATE CA	NCEL

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.

Twilio Settings		🛛 🗙
Account SID		
Auth token		
Phone		
✓ Check		
	SAVE	CANCEL

Twilio Settings dialog

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

DESCRIPTION

Backup codes are validation codes that provide users with one time access to Devolutions Password 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*.

SafeNet			
AuthAnvil			
Radius			
Vasco			
DEFAULT Default			
Google Authentica	tor	•	
Google Authentica	tor	•	
✓ Email		_	
Backup codes	🌣 Configure		

Backup Codes - Two-Factor Authentication

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

Codes list setup		×
Number of backup codes		•
	SAVE	CANCEL

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

A David Hervieux dhervieux@windjammer.net
Edit your Account
Change Gravatar
Settings
Visit our Forum
Online Help
Log Off

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 Acco	punt		×
INFORMATION ALTERNATE 2FA	Generating new backup codes invalidate any previously generated backup codes.	,	
a	Generate backup codes		
	Alternate Backup Codes		
D	26373963		
	43656568		
	76896296		
	75223482		
	95644289		
	66496839		
	34396926		
	55372679		
	28698973		
	38929365		
	79397965		
	88577384		
	SAVE	CANC	EL

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.

ADMINISTRATION > PASSWORD SERVER SETTINGS > SECURITY	H
Allowed single IPs	
Allowed masked IPs	
Denied single IPs	
Denied masked IPs	
AUTO LOCK	
Enable automatic lock account	
Attempt count	
0	

Administration - Password Server Settings - Security

IP

Allowed Single IPs	If you wish to restrain the access to the Devolutions Password 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 Password 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

	and host address) on the Devolutions Password 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

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

GeoIP Mode	Choose your method of GeoIP between: None: Will not be using GeoIP security 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 Password Server.
User ID	User ID to connect on MaxMind.
License key	License key to connect on MaxMind.
Countries	Select all authorized countries to connect to the Devolutions Password Server instance.
-----------	---

5.5.2.2.2.4 Privileged Access Management

DESCRIPTION

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

ENERAL		
Enable PAM		
CURITY		
FOLDER		
Access		
Everyone	✓ :	
CREDENTIALS		
View sensitive information on checkout		
Everyone	✓ :	
Credentials brokering		
Everyone	✓ :	
HECK OUT		
Default approval mode		
none	~	
Default reason mode		
none	~	
Default checkout time (minutes)		
20	×	

Administration - Password Server Settings - Privileged Access Management

SETTINGS

GENERAL

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

SECURITY - FOLDER

Access	Possible values : • Custom
	• Everyone
	• Never

SECURITY - CREDENTIALS

View sensitive information on checkout	Possible values : • Custom • Everyone • Never
Credentials brokering	Possible values : • Custom

• Everyone
• Never

CHECK OUT

Default approval mode	Possible values : • none
	• mandatory
Default reason mode	Possible values : • none • mandatory
	• optional
Default checkout time (minutes)	

5.5.2.3 System Permissions

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.

Password Server		😡 Windjammer IT 🗸 🗸	Ø	в
Administration > sys	TEM PERMISSIONS			
ENTRIES	ENTRIES			
MANAGEMENT	Import			
MISCELLANEOUS	Default (Disallowed)	✓ :		
TOOLS				
PAM	Export			
	Default (Disallowed)	✓ :		
	Add in root			
	Default (Allowed)	∼ :		
	Vault settings			
	Default (Disallowed)	∼ :		
	Session recording			
	Default (Disallowed)	✓ I		

Administration - System Permissions

SYSTEM PERMISSIONS

- Entries
- <u>Management</u>
- Miscellaneous
- <u>Tools</u>
- Privileged Access Management (PAM)

5.5.2.3.1 Entries

Pevolutions Password Server		😡 Windjammer IT 🗸 🗸	⊠	в
Administration > syst	TEM PERMISSIONS			E
ENTRIES	ENTRIES			
MANAGEMENT	Import			
MISCELLANEOUS	Default (Disallowed)	✓ 1		
TOOLS				
PAM	Export			
	Default (Disallowed)	✓ :		
	Add in root			
	Default (Allowed)	✓ :		
	Vault settings			
	Default (Disallowed)	✓ 1		
	Session recording			
	Default (Disallowed)	✓ :		

Administration - System Permissions

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

Devolutions Password Server		Windjammer IT 🗸	\boxtimes	B
Administration > sys	TEM PERMISSIONS			
ENTRIES	MANAGEMENT			_
MANAGEMENT	Users			
MISCELLANEOUS	Default (Disallowed)	✓ :		
TOOLS				
PAM	Roles			
	Default (Disallowed)	✓ :		
	Vault			
	Default (Disallowed)	✓ I		
	Systems settings			
	Default (Disallowed)	✓ :		
	Templates			
	Default (Disallowed)	✓ :		
	Password templates			
	Default (Disallowed)	✓ :		
	Default (Disallowed)	✓ :		

Administration - System Permissions - Management

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

Password Server		Windjammer IT	~ 🛛	в
Administration > sys	TEM PERMISSIONS			
ENTRIES	MISCELLANEOUS			
MANAGEMENT	Activity logs			
MISCELLANEOUS	Default (Disallowed)	~		
TOOLS				
PAM	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

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

5.5.2.3.4 Tools

Devolutions Password Server	😡 Windjammer IT 🕞 👻	🖂 时
Administration > sy	/STEM PERMISSIONS	E .
ENTRIES	TOOLS	
MANAGEMENT	Built-in tools (Wake On Lan, NetStat, Ping,)	
MISCELLANEOUS	Default 🗸	
TOOLS	Macro/Script/Tool entry	
PAM	Default v	
	Remote tools	
	Default 🗸	
	Web management tools	
	Default 🗸	
	Console management tools	
	Default (Disallow)	

Administration - System Permissions - Tools

Buit-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.
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 <u>Privileged Access Management</u> in the **Password Server Settings**.

Devolutions Password Server	ໜ Windjammer IT 🛛 👻	🖂 🕞
Administration > Sy	STEM PERMISSIONS	H
ENTRIES MANAGEMENT MISCELLANEOUS TOOLS PAM	PRIVILEGED ACCESS MANAGEMENT Has Access To The PAM Section Default (Disallow) Manage Privileged Accounts Default (Disallow) Privileged Access Management Configuration Page	

Administration - System Permissions - PAM

Has Access to the PAM Section	Determine who has access to the PAM section.

Manage Privileged Accounts	Determine who can managed the Privileged accounts.
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.

≡	Password Server	My Private Vault 🗸 🗸	🛛 🛑
Ø	ADMINISTRATION > PASSWORD TEMPLATES		+ 0
۲	Name *	Description 🗢	
P	Strong Policy	Advanced settings	/ 🖻
୍	III Export	H 4 1 > H	1 Results
☆			
5			
毘			

Administration - Password Templates

Password Templates				2 × 12
SECURITY			PREVIEW	
Name			Password Count	
Strong Policy			30	▲ ▼
Mode				
Advanced settings		~		<u>^</u>
Password length				
20		▲ ▼		
 ✓ Upper-case (A, B,) ✓ Underline (_) High ANSI characters Minus (-) Brackets ([,], (,), <>) 	2 ▲ ✓ Digits (0, 1, 2,) 0 ▲ ✓ Special (!, \$, %, &,) 0 ▲ ✓ Lower-case (a, b, c,) 0 ▲ Space () 0 ▲ XML Compliant			~
Include the following character A Exclude the following charact #,\$,<,i,I	ers 1	×		
				UPDATE CANCEL

Password Templates

Name	Name of the Password Template.
Mode	• Default
	Advanced settings
	Readable password
	• Use a pattern
	Pronounceable password
	Strong password
Upper-case (A, B, C,)	Will include uppercase letters for password generation.
Underline (_)	Will include the underline (_) character for password generation.

High ANSI characters	Will include characters form '-' 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.
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		+ 2
Name 🔶	Туре	
MyFolderTemplate	Group	â 🖊 🛍
MyRDPTemplate	RDPConfigured	i 🖉 🖉 💼
CtherFolderTemplate	Group	e 🖉 💼
III Display value only	H 1 ⊨ H	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.

=	Devolutions Password Server	🚾) Windjammer IT 🛛 🗸	M 🖬
Ø	Administration > backup manage	ER	ii <i>i</i>
⊛ ₽ 0 €	DATABASE CONFIGURATION Enable database backup Backup database file path WEB CONFIGURATION		
	Enable web backup Backup web file path		
	Notify Administrator on backup f Backup start time 11/13/2018 Repeat every Days Hot 0 1 ADVANCED	siled 143 AM rs ***	
	Database backup SQL timeout (Min 1 Keep number of backups 1 Copy only database backup	tes)	

Administration - Backup Manager

SETTINGS

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

Enable database backup	Activate the backup of the SQL database.
Backup database file path	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. 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.

WEB CONFIGURATION

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

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 <u>Email</u> <u>Settings</u> .

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

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 ≣ Display value only ▼	Database backup co	C:\Users\Administrat	C:\Users\Administrat 5 ▶ ▶	1274 Results

Administration - Backup List

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	A check mark will indicate a successful backup. An X will indicate that the backup has failed.

5.6 Role Based Security

Devolutions Password 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 Password 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 Password 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.

≡	Devolutions Password Server		⊠ 🛑		
Θ	ADMINISTRATION > ROLES			+	4 C
۲	Name *	Description 🗢	Role Type	Is administrator	
P	Show-Corporate	Azure/Office365	Office365		🎨 🖌 🟛
O,	Show-IT Corp	Azure/Office365	Office365		🎨 💉 🟛
☆	WINDJAMMER\Help Desk		Active Directory		🎨 🥒 🟛
195	WINDJAMMER\HR		Active Directory		🎨 🖌 🟛
	WINDJAMMER\RDM Admins	Full administrators	Active Directory	~	🎨 🖌 🟛
185	WINDJAMMER\RDM Help Desk	Help Desk Staff	Active Directory		🎨 🖌 🟛
	WINDJAMMER\RDM Service De	Service Desk Staff - IT Depart	Active Directory		🍪 🖌 🟛
	WINDJAMMER\Service Desk		Active Directory		🍪 🖌 🟛
	WINDJAMMER\Vault - Admins		Active Directory		🍪 🖌 🟛
	WINDJAMMER\Vault - Corporate	CAL Non-IT Users	Active Directory		🎨 🖊 🟛
	III Export		∺ < 1 2 ▶ H		13 Results

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	*
	ОК	CANCEL

Configure a Role

To assign users to the role, click 记, 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 Password Server.

Role Assignment - Service Desk			
🗙 Unselect All 🗸 Select All			
Name 📤	Description	Is administrator	ls member
_Administrator		~	
bill@windjammer.loc	Bill Preston	~	
	H 4 1 ► H		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	2	•
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	GENERAL Authentication type Custom (Devolutions) User • Password • User type Read only user User license type Read only user Default 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 Password Server.

GENERAL INFORMATION	Only custom roles can be manually assigned.						
TWO FACTOR ROLES	🗙 Unselect All 🛛 🖌 Sele	ect All					
APPLICATIONS	Name 📤	Description	Role Type 🗢	Is member			
VAULTS	WINDJAMMER\Vault	Password Vault Users	Active Directory				
EMAIL NOTIFICATIONS	WINDJAMMER\Vault		Active Directory				
	WINDJAMMER\RDM S	Service Desk Staff - IT	Active Directory				
	Show-IT Corp	Azure/Office365	Office365				
	WINDJAMMER\Vault	Groups from IT Depa	Active Directory				
	Show-Corporate	Azure/Office365	Office365				
	WINDJAMMER\RDM	Full administrators	Active Directory				
	WINDJAMMER\Vault	CAL Non-IT Users	Active Directory				
	WINDJAMMER\HR		Active Directory				
	WINDJAMMER\Servic		Active Directory				

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.

Add user		🛛 🗙
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	GENERAL Authentication type Domain User • david@windjammer.loc User type User type Administrator Must change password at next logon INFORMATION First name Last name	✓ ✓ Enabled
	Email • david@windjammer.loc	
		ADD CANCEL

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.

 \checkmark Set up manually which rights are granted to the user.

Add user		x
GENERAL INFORMATION TWO FACTOR ROLES APPLICATIONS VAULTS SETTINGS EMAIL NOTIFICATIONS	GENERAL Authentication type Domain User • ted@windjammer.loc User type Restricted user User license type Default Change password at next logon RIGHTS	^
	Add Edit Add in root Move INFORMATION First name Email • ted@windjammer.loc	~
	ADD CANC	EL

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					2	×	
GENERAL MORE	Permission Default				~	^	
SECURITY	GENERAL	SECURITY	MORE	ATTACHMENTS	DOCUMENTATION	1	
INTERFACE	View						
EMAIL	Inherited				\sim		
NOTIFICATIONS ADVANCED	Roles: WINDJAMMER\RDM Service Desk						
	Edit						
	Inherited (Never)						
	Delete						
	Inherited (Never)						
	View password						
	Inherited (Never)						
	Connect (Execute)						
	Inherited (All	owed)			\sim		
					UPDATE CANO	TEL	

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					2	×
GENERAL SECURITY	 PERMISSIONS Allow offline True Add in root Never Root properties Never Permission Never GENERAL View Default Add Default Edit Default 	SECURITY	MORE	ATTACHMENTS	DOCUMENTATION	
					UPDATE CANO	CEL

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 <u>System Permissions</u>.

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

Folder - Work	station				×
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Permission GENERAL SECURITY MORE View Everyone Add Custom Add Custom Edit Custom 4 Edit Custom Edit Custom 4 Edit Custom 4 Edit Custom View 2 Edit Custom 4 Edit Custom Custom 4 Edit Custom Custom View Password Custom Custom Custom Roles: WINDJAMMER\Vault - IT Corp Execute Default View Password Custom Execute Default Default View Password Password	ATTACHMENTS		• TION : : : :	<
			UPDATE	CANCE	EL

Permissions Panel

1. Permission	Sets the permission mode. This must be set to Custom in order to change the discrete permissions below. Select between:
	 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.

	 Never: no one but the administrators will be granted the permissions
2. Discrete permissions	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:
	• 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	Lets you select Users / Roles to be granted the permission. Available only if the permission is set to Custom .
4. Current permission	Displays the granted permission for the current entry.

GENERAL

Folder - Works	station						×
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Permission Custom GENERAL View Everyone Add Custom Roles: WINDJAI Delete Default View password Custom Roles: WINDJAI Delete Default	SECURITY MMER\Vault - IT Cor MMER\Vault - IT Cor	MORE	ATTACHMENTS	DOCUMENTA	TION	~
					UPDATE	CANCE	¥

Permissions - General

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.

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

SECURITY

Folder - Work	station						×	
GENERAL MORE SECURITY	Permission Custom	CECUPITY.	11005		DOCUMENT	•	~	*
USER INTERFACE EMAIL NOTIFICATIONS	Edit permission Default	IS	MORE	ATTACHMENTS		:		
ADVANCED	Entry history Default Password histo	ry			•			
	Default				UPDATE	CANC	FI	

Permissions - Security

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 - Work	station					2	×
GENERAL MORE SECURITY	Permission Custom					•	~
USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	GENERAL Remote tools Default Inventory	SECURITY	MORE	ATTACHMENTS		ion	
	Default				UPDATE	CANCE	v EL

Permissions - More

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

ATTACHMENTS

Folder - Work	station						×
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Permission Custom GENERAL View attachme Default Add/edit/delet Default	SECURITY ents te attachments	MORE	ATTACHMENTS	DOCUMENT/	► ATION	~
					UPDATE	CANCE	EL

Permissions - Attachment

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

DOCUMENTATION

Folder - Work	station						×	
GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Permission Custom GENERAL View document Everyone Edit documenta Default	SECURITY ation	MORE	ATTACHMENTS	DOCUMENT/	► ATION	^	
					UPDATE	CANCE	EL	

Permissions - Documentation

View documentation	Allow users/roles to view documentation.
Edit documentation	Allow users/roles to edit documentation.
Privileged Access Management

Part VI

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 Password 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 sidepanel appear on the left.

ADMINISTRATION > PASSWORD SERVER SETTINGS > PRIVILEGED ACCESS	
GENERAL	Save
C Enable PAM	
SECURITY	
FOLDER	

Enabling PAM

3. Configure the default settings for the <u>checkout system</u>, <u>credentials brokering</u>, <u>sensitive information access</u>, default checkout times and synchronizations. The **Custom** setting allows role-based access control.

FOI DED	
FOLDER	
Access	
Everyone	∼ :
CREDENTIALS	
View sensitive information on checkout	
Everyone	✓ :
Credentials brokering	
Everyone	✓ :
HECK OUT Default approval mode	
HECK OUT Default approval mode	
HECK OUT Default approval mode mandatory	~
HECK OUT Default approval mode mandatory Default reason mode	~
HECK OUT Default approval mode mandatory Default reason mode optional	~
HECK OUT Default approval mode mandatory Default reason mode optional Default checkout time (minutes)	~
HECK OUT Default approval mode mandatory Default reason mode optional Default checkout time (minutes) 240	✓
HECK OUT Default approval mode mandatory Default reason mode optional Default checkout time (minutes) 240 (NCHRONIZATION	✓
HECK OUT Default approval mode mandatory Default reason mode optional Default checkout time (minutes) 240 VNCHRONIZATION Check synchronization status every (minutes)	✓

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**.

DMINISTRATION > SYS	TEM PERMISSIONS		
ENTRIES	PRIVILEGED ACCESS		
MANAGEMENT MISCELLANEOUS	Has Access To The PAM Section		
TOOLS PAM	Users: kelly@windjammer.loc,maurice@windjammer.loc,bob@windjammer.loc		
	Manage Privileged Accounts Default (Disallow)	✓ 1:	

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.

ENERAL			
Name •			
PAM Provider			
OMAIN			
Domain name		User logon type •	
windjammer.loc	+	Sam Account Name	~
Protocol •		Port	
LDAP	~	636	
L		L3	
Make sure you keep retrieve it later. Username •	o a copy of	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme	o a copy of er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme User Principal Name •	o a copy of er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme User Principal Name • pam_access@windjamme	er.loc er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username pam_access@windjamme User Principal Name pam_access@windjamme Password	er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme Dam_access@windjamme pam_access@windjamme Password ••••••	er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme pam_access@windjamme pam_access@windjamme Password ••••••	er.loc	the password, you will not I	be able t
Make sure you keep retrieve it later. Username pam_access@windjamme pam_access@windjamme pam_access@windjamme Password ••••••	er.loc	the password, you will not	be able t
Make sure you keep retrieve it later. Username • pam_access@windjamme Deam_access@windjamme Password •••••• CTIONS	er.loc	the password, you will not I Test Co	be able t
Make sure you keep retrieve it later. Username pam_access@windjamme Dam_access@windjamme pam_access@windjamme Password •••••• CTIONS Add Team Folder Add Scap Configuration	er.loc	the password, you will not I Test Co	be able t
Make sure you keep retrieve it later. Username pam_access@windjamme Dam_access@windjamme pam_access@windjamme Password •••••• CTIONS Add Team Folder Add Scan Configuration	er.loc er.loc	the password, you will not	be able t

PAM Provider Configuration

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*.

Scan Configuration	×
GENERAL	
Name	
ShowcaseOU20	*
CONFIGURATION	
Provider	
PAM Provider	~
Domain name	
windjammer.loc T	+
Domain container	
OU=Belfast,OU=Domain Accounts,DC=windjammer,DC=l	oc +
SCHEDULE	
Recurrence	
ACTIONS	
Start Scan on Save	
ОК	Cancel

PAM Scan Config

For more information, please refer to the <u>Scan Configurations</u> 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 <u>folder's security options</u> if you don't want to give them the defaults you set during the initial configuration. You can also <u>customize the approvers on the folder</u> directly which will give you a list of the administrators.

E Devolutions Password Server	🔓 My Private Vault 🗸 🗸	🛛 🔤
Dashboard	PRMLEGED ACCESS > PRIVLEGED ACCOUNT MANAGEMENT	83 + •
Q Search		Fiter by name and tax
☆ Favorites	V FOLDERS	
🕑 Vaults	Global PA Folder Folder Manage OU10 Folder Folder Manage OU12	Manage OU14 Folder
Privileged Access	Manage OU20 Rolder Service Accounts	
	* ACCOUNTS	
	No data to display	

PAM Create Folder

IMPORT ACCOUNTS FROM A SCAN

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

P	RIVILEG	ED ACCESS > ACCOUNT DISCOVERY						(¢;
	Status	Name	Scan Type	Last Run Time	Next Run Time	Recurrent	Results	
	~	ShowcaseOU14	Domain	2020-01-20 17:05			3	ூ⊘∕∎
	~	ShowcaseOU12	Domain	2020-01-20 16:23			3	/iew Result
	~	ShowcaseOU20	Domain	2020-01-20 17:10			3	o 💿 🗶 💼
	~	ShowcaseOU10	Domain	2020-01-20 17:05			3	ூ⊘∕∎

View Scan Results

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

PRIV	EGED ACCESS > ACCOUNT DISCOV	/ERY > SHOWCASEOU20				Filter	Import Selected Accounts
_	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
	_financialsmgr20@windjamm	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.

Import		×
IMPORT 1 USER(S)		
Provider		
Pam Manager		~
Folder		
/Manage OU20		~
 Reset Password On Import 		
Reset Password On Check-In		
	ÖK	Cancel

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 Password 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.

PRIVILEGED ACCESS > PRIVILEGED ACCOUNT MANAGEMENT	\$\$ + 🖬
A >	Filter by name and tag
▼ FOLDERS	
SSH Folder Telemark Folder Folder Windjammer Folder	
✓ ACCOUNTS	
No data to display	

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 ACCESS > PRIVILEGED ACCOUNT MANAGEMENT		:	833	+	4
☆ ACCOUNTS		Filter by nat	me a	nd tag	
bomain User	 Check Out Check Out Check Out Reset Password Schedule Check Synchronization Status Password history Delete Logs 				

Privileged Accounts folder content

MORE

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

Status	
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.

Pevolutions Password Server	👸 My Private Vault 🗸 👻			🖂 🖂	
(2) Dashboard	PRIVILEGED ACCESS > PRC	VIDERS			+ C
O Search	Name 🔺	Туре 🗢	Domain\Host 🗢	Scan Configurations 🗢	
Favorites	Provider - Downhill	Domain User	downhill.loc	Downhill Scan	🖋 🕸 🖨 💼
2	Provider - Windjammer	Domain User	windjammer.loc	Windjammer scan	🖋 🕸 🛱 💼
🛞 Vaults	SSH Provider	Local User	192.168.7.2	SSH Scan	🖋 🕸 🖨 💼
🐌 My Private Vault		И	< 1 → H		3 Results
Privileged Access					
🖺 Reports					
Administration					
Online Help					

Providers dashboard

On the creation of a Provider, two choices are available: <u>Domain User</u>, <u>SSH Local User</u>, and <u>SQL User</u>. Multiple Providers can be created and can reach different domains as long as the Devolutions Password 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.

E Pevolutions Password Server	💫 My Private Vault 🗸 👻			🖂 🖂	
(2) Dashboard	PRIVILEGED ACCESS > PRO	VIDERS			+ C
Search	Name 🔺	Туре 🗢	Domain\Host 🗢	Scan Configurations 🗢	
Favorites	Provider - Downhill	Domain User	downhill.loc	Downhill Scan	🖋 🕸 🛱 💼
~	Provider - Windjammer	Domain User	windjammer.loc	Windjammer scan	🖋 🕸 🗘 💼
(*) Vaults	SSH Provider	Local User	192.168.7.2	SSH Scan	🖋 🕸 🔃 💼
My Private Vault		И	∢ 1 → H		3 Results
Privileged Access					
Reports					
Administration					
Online Help					

Providers dashboard

On the creation of a Provider, three choices are available: <u>Domain User</u>, <u>SQL Server</u> or <u>SSH Local User</u>. Multiple Providers can be created and can reach different domains as long as the Devolutions Password Server instance can communicate with the domain controller.



Provider Type dialog

6.3.1 Domain Provider

DESCRIPTION

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

rovider				2	;
GENERAL					
Name •					
Provider - Windjamme	r]
DOMAIN					
Domain name					
windjammer.loc				+	
Protocol •	Po	ort			
LDAP	~				
REDENTIALS Make sure you ke retrieve it later. Username •	eep a copy of the	password, y	vou will not	be able to	
administrator@windja	mmer.loc				J
Password					
•••••				⊕ :	

Domain Provider dialog

GENERAL

Name	Display name of the Provider.

DOMAIN

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:
	• LDAP
	• LDAPS
Port	Set the port number used with the configured Protocol.

CREDENTIALS

Username	Username of the domain account.
Password	Password of the domain account.

6.3.2 Local SSH Provider

DESCRIPTION

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

Provider	X 12
GENERAL	
Name •	
SSH Provider	
HOST	
Host	
192.168.7.2	
Port	
22	
CREDENTIALS Make sure you keep a copy of the password, you retrieve it later.	ı will not be able to
Username •	
MyUsername	
Password	
•••••	⊕ :
	Test Connection
	Save Cancel

SSH Provider dialog

GENERAL

Name	Display name of the Provider.

HOST

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

CREDENTIALS

Username	Username of the SSH account.
Password	Password of the SSH account.

6.3.3 SQL Server Provider

DESCRIPTION

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

Provider	2	×
GENERAL		_
Name •		- 11
SQL Provider		- 11
SERVER		_
Server name •		- 11
windjammer.loc\SQL2016		- 11
	Advanced	- 11
CREDENTIALS Make sure you keep a copy of the password, you w retrieve it later.	ill not be able to	
Username •		
sa		- 11
Password		
•••••	⊙ :	
	Test Connection	
	Save Ca	ancel

SQL Provider dialog

GENERAL

Name	Display name of the Provider.

SERVER

Server	Hostname of the SQL Server

CREDENTIALS

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.

Pevolutions Password Server		🐞 My Priv	vate Vault 💙				M 🖪
Dashboard	PRIVILEGED ACCESS > ACCOU	INT DISCOVERY					¢
C Search	Status Name	Scan Type	Last Run Time	Next Run Time	Recurrent	Results	
Favorites	Downhill Scan	Domain	2019-12-13 4:00 PM			41	🗢 🔘 🖊 💼
A	Vindjammer scan	Domain	2019-05-24 11:27 AM			22	👁 🔘 🖊 💼
🛞 Vaults	SSH Scan	Local Accounts	2019-12-13 4:00 PM				• () 🖉
😰 My Private Vault			N 4 1 ► N				3 Results
Privileged Access							
Reports							
Administration							
Online Help							

Account Discovery dialog

On the creation of an Account Discovery, it is possible to choose between <u>Domain</u>, <u>SQL</u> <u>Server</u> or <u>SSH Local Accounts</u>.

Select Acco	ount Discove	ery Type 🗙
Domain	SSH Local Accounts	SQL
		Cancel

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.

Bevolutions Password Server	🔓 My Private Vault 👻	
(2) Dashboard	PRIVILEGED ACCESS > ACCOUNT DISCOVERY > DOWNHILL SCAN	
Search	Filter	
S Eavorites		
	dbrunner2@down DOWNHILL\dbrun dbrunner2 DBRunner2 downhill.	DC
🛞 Vaults	pedro@downhill.loc DOWNHILL\pedro pedro Pedro downhill.l	oc
😰 My Private Vault	roaming@downhil DOWNHILL\roami roaming Roaming user downhill.i	oc
	duo@downhill.loc DOWNHILL\duo duo Duo downhill.l	ж
Privileged Access	downtest@downh DOWNHILL\downt downtest downtest downtest	oc
	DisableMeTest@d DOWNHILL\Disabl DisableMeTest DisableMe Test downhill.	oc
P. Departs	test@downhill.loc DOWNHILL\test test downhill.l	oc
E Reports	testhubert@down DOWNHILL\testhu testhubert Hubert downhill.l	ос
Administration	test1@downhill.loc DOWNHILL\test1 test1 test1 test1 test1@downhill.co downhill.l	oc
Online Help	aroy@downhill.loc DOWNHILL\aroy aroy Alexandre Roy downhill.l	oc
	H 4 1 2 → H	,

Account Discovery results dialog

In order to manage privileged accounts with the Devolutions Password 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.

🙆 Dashboard	PRIVILEGED ACCESS > ACCOUN	IT DISCOVERY > DO	WNHILL SCAN			E
0	walter@downhillp D	OWNHILL\walter	walter	Walter	Harp	downhill Import Selected Accounts
Search	✓ TestE@downhill.loc D	OWNHILL\TestE	TestE	TestQ		downhill.loc
Stavorites	✓ Hpotter@downhill D	OWNHILL\Hpotter	Hpotter	Harry	Potter	downhill.loc

Import Selected Accounts operation

On import, the <u>Provider</u>, Destination Folder and Reset Password options can be set.





IMPORT

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 Password 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 Unit
1 Minutes Hours Days
ACTIONS
Start Scan on Save
OK Cancel



GENERAL

Name	Display name of the Domain Account Discovery.

CONFIGURATION

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

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

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 Password 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 Unit	
1 Minutes Hours Days	
ACTIONS	
Start Scan on Save	
ОК Са	ncel

SSH Account Discovery dialog

GENERAL

Name	Display name of the SSH Account Discovery.

CONFIGURATION

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

SCHEDULE

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

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 Password Server to scan the host to find accounts. The accounts will not be automatically added.

Scan Configuration X	
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

Name	Display name of the SQL Account Discovery.

CONFIGURATION

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

SCHEDULE

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

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 Password Server's webpage.

2. The user then clicks on the *Accounts* panel.

Pevolutions Password Server		🔓 My Private Vault 🗸 🗸	🖂 📧
Dashboard	PRIVILEGED ACCESS		
O Search	Accounts 🖸 🛛 🗘		
5Å Favorites	2 25		
Vaults	Accounts		
😰 My Private Vault	Checkouts 🖸	Pending (0) Active (0) C Recent Activities [2] All (0) Mine (0)	C
Privileged Access	There are no pending checkouts.	There is no logs	

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.

Pevolutions Password Server	🔒 My Private Vault 🐱	M 🙆
Dashboard	PRIVILEGED ACCESS > PRIVILEGED ACCOUNT MANAGEMENT	
C Search	☆ > Manage OU20	Filter by name and tag
☆ Favorites	*ACCOUNTS	
 Vaults My Private Vault 	Domain User Image: Second Se	
Privileged Access		

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	2	×
Reason (Optional)		
I need to checkout this account to access a secure server. Please approve	2.	
Duration (in minutes) Approver		
60 Bob Anderson		~
Request checkout	С	lose

Checkout Request

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

E Pevolutions Password Server			🧓 Windjammer Defa 👻	,		X (9	A
Dashboard	PRMLEGED ACCESS					Q. (1
O Search	Accounts 🖸	0	Providers	0	Scan Configurations	C	
🗙 Favorites		25		2		6	
Vaults		Accounts	U	Providers	\bullet	Scan Configurations	
🐌 My Private Vault	Checkouts 단		Pending (1) Active (0)	Recent Activities 🖸		All (0) Mine (0)	
Privileged Access	Kelly Slater Requested By 2020-03-04 14:27		nux_account20 Approver Bob Anderson	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 Password Server's webpage.

2. The user then clicks on the Accounts panel.

E Devolutions Password Server		😰 My Private Vault 👻	🖂 📧
Dashboard	PRIMLEGED ACCESS		
Search	Accounts 🖸	0	
☆ Favorites		25	
Vaults	Acc	nts	
My Private Vault	Checkouts 년	Pending (0) Active (0) C Recent Activities C All (0) Mine (0)	C
Privileged Access	There are no pending checkouts	There is no logs	
	• mere are no pending checkouts.		

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.

E Devolutions Password Server	🔓 My Private Vault 🗸 🗸	🖂 🔞
Dashboard	PRVILEGED ACCESS > PRVILEGED ACCOUNT MANAGEMENT	
Q Search	Anage OU20	Filter by name and tag
₩ Favorites	*ACCOUNTS	
 Vaults My Private Vault 	Desclupoperator20 Image: Second	
Privileged Access		

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	2	×
Reason (Optional)		
I need to checkout this account to access a secure server. Please approve		
Duration (in minutes) Approver		
60 Bob Anderson		~
Request checkout	С	lose

Checkout Request

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

Pevolutions Password Server			🚾 Windjammer Defa 🗸	,		🖂 😣
Dashboard	PRMLEGED ACCESS					Q (1
🔍 Search	Accounts 🖸	C	Providers 🖸	0	Scan Configurations	0
🗙 Favorites		25		2		6
Vaults		Accounts		Providers	\bullet	scan conigurations
My Private Vault My Private Vault	Checkouts E2		Pending (1) Active (0) C nux_account20 Approver Bob Anderson	Recent Activities [2]		All (0) Mine (0)

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	
Duration (in minutes)	
60	
Approver Message	
Approve Deny Clo	se

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 :

Check	Out - Active	00:58:22	2 ×
	•••••	1	
		Checkin	Close

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.

Check Out - Active	00:05:41 🏼 🗶
UEAfzES!e59c!jUo^PT3	
	Checkin Close

Check	Out - Active	00:0	5:53 🖥	× 1
	•••••			
		с	heckin	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.

Remote Desktop Manager - Check Out -	_financialsmgr ialsmgr	×
Duration (in minutes)	Approver Bob Anderson (bob@windjammer.loc)	•
Reason		
	OK Canc	el

Credential Brokering Checkout Request

Devolutions Web Login

Part VII

7 Devolutions Web Login

7.1 Overview

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.

		گر
Remote Desktop Manager	Devolutions Password Server	Devolutions Password Hub
Centralize, Manage and Secure Remote Connections	Secure, Manage and Monitor Access to Privileged Accounts	Vault and Manage Business-User Passwords
Remote Desktop Manager centralizes all remote connections on a single platform that is securely shared between users and across the entire team.	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

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

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:

- <u>Chrome</u>
- Firefox
- <u>Microsoft Edge</u>
- Opera

7.2.1 Chrome

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

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 <u>Devolutions Web Login</u> 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

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 <u>Devolutions Web Login</u> website page to the Chrome Web Store.
- 6. Click Add to Chrome.

🚡 chrome v	web store
Home >	Extensions > Devolutions Web Login
*	Offered by: https://devolutions.net **** * 23 Productivity 14.590 users
	Overview Reviews Support Related

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

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 <u>Devolutions Web Login</u> 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.

← ★ Devolutions Web Login	
	Install
Description Form filler that obtains entries from Remote Desktop Manager and Devolutions Password Server	
Version 2019.2.0.0	
Size 11.6 MB	
Permissions Read your browsing history Communicate with cooperating native applications	
Site access	
Automatically allow access on the following sites	Can access.
Allow in incognito	
Allow access to file URLs	
Allow access to search page results	
Source Not from Opera add-ons.	
Remove extension	

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

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.

 Choose Devolutions Password Hub in the list and Save. You could at this point import settings; the option will also be available in the <u>Settings</u> 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.

Devolu	tions
Log in to c	ontinue
Password	
Contin	ue
Forgot Password	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.



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.

8	Bob Anderso	n
ф,	Settings	
0	About	>
<u>ک</u>	Log Off	

Devolutions Web Login About

3. Validate the Password Hub URL.

<	Back About	
· Te	Bob Anderson bob@windjammer.co Log Off	
٢	https://windjammer.devolutions.app	
ഹ	Visit our Forum	
	Online Help	
*		

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.

	Bob Anderson
Ф,	Settings
1	About
ŧ	Log Off

Devolutions Web Login Settings

3. Click *HUB*.



Devolutions Web Login Settings Menu

4. In the *General* section, click *List*.

General			
Enable Devolutions Password Hub			
Server UR	L		List
https://	windjammer	.devolutions.app	

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.



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.



Password Hub Switch Master key

7.3.2 Password Server

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.



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 <u>Settings</u> menu after the log in.



First Login

3. Enter the server address. Test the connection to validate it, then Save.



Server Address

4. Press the *Log In* after you saved the address.



Devolutions Web Login Login

5. Enter your Devolutions Password Server credentials and log in.

Log in to you	tions rd Server
Username	*
Password	*
Log Ir	
	v 2019.1.20.0

Devolutions Password Server Login

Devolutions Web Login is now connected to your vaults.



Devolutions Web Login Connected

7.3.3 Remote Desktop Manager

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.



 Choose *Remote Desktop Manager* in the list and *Save*. You could at this point import settings; the option will also be available in the <u>Settings</u> menu after the log in.



First Login

You will be automatically connected to your vaults.

7	ilter	0
	$\langle \! \! \! \! \rangle$	
	No credentials available for this site	
+	Add Website	
*	Password Generator	>
Ф,	Settings	
0	About	>

Devolutions Web Login Connected

7.4 Exploring Devolutions Web Login

7.4.1 Menu

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 private 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

Devolutions Web Login settings are separated in two categories, <u>Configuration</u> and <u>Data sources</u>.

Devolutions Web Login			
Settings			
Configuratio	n		
General	Never List	Import / Export	
Data sources	4		
RDM	DPS	НИВ	

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 <u>Remote Desktop Manager</u>, <u>Devolutions Password Server</u> and <u>Devolutions</u> <u>Password Hub</u>.

REMOTE DESKTOP MANAGER

GENERAL OPTIONS	DESCRIPTION	
Enable Remote Desktop Manager app	Retrieve entries from Remote Desktop Manager when the application is open.	
Use default port (19443)	Communicate with the default port 19443 between the application.	
Add entry in private vault by default	Save new entries in the private vault.	
Destination folder	Choose the folder where the credentials are stored in the vault.	

ACTION OPTIONS	DESCRIPTION	
Automatically retrieve credentials on page load	Devolutions Web Login automatically search for credentials in the data source when connecting to a website. If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.	
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	Secure the port with an application key by using the same code in Remote Desktop Manager and Devolutions Web Login. Navigate to <i>File – Options – Browser</i> <i>Extensions</i> in Remote Desktop Manager to set the application key	
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	

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	Devolutions Web Login automatically search for credentials in the data source when connecting to a website. If disabled, click on the Devolutions Web Login extension icon to manually retrieve credentials.	
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

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.

Devolut	ions
Log in to co	ontinue
bob@windjammer.co	(k)
Password	(K)
Continue	e
Forgot Password Create Account	

Automatic Log In

7.4.2.1 Remote Desktop Manager

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.
E Remote Desktop Manager	[Customer Success]				•	×
Information						
General More Password Management Security Settings User Interface Information Events Advanced	Name Folder Display	Embedded (tabbed)	•			
	Website Website Credentials Username Domain Password	Equivalent URLs Default		•		
Website	Compare type	ser extension link Default	Security One Tim More Se	<u>Questions</u> e Password Settings (OTP) ttings		
E Variables	Search property	n	Create another	ОК	Cano	cel

Enable web browser extension link

7.4.3 Secure Devolutions Web Login

As mentioned in the Devolutions Web Login <u>Overview</u> 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			×
 ✓ General Application Start Application Close Notification Proxy (Web) Custom Variables > User Interface > Types Reports Browser Extensions Key Agent Security > Tools Path Cloud > Advanced 	Devolutions Web Login (Browser Extensions)		
Mark Import Options			
Export Options			
	Search property OK	Cance	el 🛛

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		
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

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.

Log in to your accou	int
Username	k
Password	X
l se le	

One Credential Login with Devolutions Web Login

Devolutions Launcher

Part VIII

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.

	<mark>ж</mark>
Devolutions Password Server	Devolutions Password Hub
Secure, Manage and Monitor Access to Privileged Accounts	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 <u>Devolutions Launcher</u> or search the companion tools in the products section of <u>Devolutions</u>.



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	×
Configure Shortcuts Create application shortcuts	53
Create shortcuts for Devolutions Launcher in the following locations:	
☑ Desktop	
Start Menu Programs folder	
Startup folder	
Quick Launch toolbar	
Advanced Installer	Cancel

Devolutions Launcher Setup Wizard - Configure Shortcuts

6. Accept the terms of the license agreement and click Next.

Devolutions Launcher Setup	>		
End-User License Agreement Please read the following license agreement o	carefully		
END USER LICENS	SE AGREEMENT		
Devolutions [®] Launcher			
This End User License Agreement applies to D	EVOLUTIONS [®] LAUNCHER.		
• I accept the terms in the License Agreeme	ent		
\bigcirc I <u>do</u> not accept the terms in the License A	Agreement		
Advanced Installer			
	< Back Next > Cancel		

Devolutions Launcher - End User License Agreement

7. Click Install.

Ready to Install The Setup Wizard is ready to begin the installation Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.	
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.	
Advanced Installer	

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 <u>Devolutions Launcher</u> or search the companion tools in the products section of <u>Devolutions</u>.
- 2. Open the downloaded file.
- 3. Drag the Devolutions Launcher icon into the application folder.



8.2.4 Android

Follow these steps to install Devolutions Launcher:

- 1. Download the <u>Devolutions Launcher</u> 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*.

VANCED	
oken Valid Time (minutes)	
1440	-
nactivity time (minutes)	
20	
Jser license type	
Default	
aunch connection with	
Default	
Default	

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			×
Landing page			
Launch connection with			
Default			•
Default RDM			
Devolutions Launcher			
Default			•
	SAVE	CANC	EL

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.

Authentication		×
E	Devolutions Password Server	
	Cancel 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**.

Authentication	×	
E	Devolutions Password Server	
Username		
Password		
	Cancel Next	

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.

<section-header> Settings</section-header>	×	
General Source Logs About	RDP Use ActiveX Theme Theme Light Languages	
	Language English (United States)	

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.

<section-header> Settings</section-header>		×
General Source Logs About	Logs Log path C:\Program Files (x86)\Devolutions\Devolu Show logs Send Error Report	
	Save Cance	2

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.

		Settings			
(General	Login	Logging		
		B			
		DPS			
				Close	Save

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**..

	Enter Credentials
	Devolutions Password Server
Username	
Password	
	Cancel Next

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.

\bullet \circ \circ	Settings
	General Login Logging
Appearance	
Theme	Light
Language	
Language	English
	Close Save

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.

•••		Settings		
	General	Login	Logging	
Logging				
Loo outh				
Log path				
				Show logs
				Close Save

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.

• •	Help and Support		
5.7	Launcher Version 2019.1.3.0 Online Help Visit Our Forum Open Website		
	Send Error Report		
	Open Source		
	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.



1. Choose *Devolutions Password Server*.

÷	Web Source Selection
	Baba Hub
	DPS

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**.

Authentication		
Devolutions Password Server		
Username		
Password		

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.

Web Source Selection
<u> </u>
Hub
DPS
Sessions 😫 Login 🔅 Settings 🚱 Help And Support

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**.

KWeb Source Selection	Authentica	tion		Next
)evolu Passwo	ition ord Se	s erver	
Username				
Password				
	0			
Sessions	O Login Q	Seconds 6	Help And Support	



Secure the application with a password in **Settings - Security**. Once registered, there is no way to recover the password.

DEVOLUTIONS LAUNCHER MENU

Sessions	Account	🔇 Open DPS	C Settings	Help And Support
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	
Log in to continue	
Password	
Continue	
Forgot Password Create Account	

Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub masterkey and click *Next*.

thentication			×
ക്	Devolutions Hub		
Master key			
		Next Cancel	

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.

<section-header> Settings</section-header>	×
General Source Logs	RDP Use ActiveX
About	Theme Theme Light •
	Language English (United States)
	Save Cancel

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.

<section-header> Settings</section-header>	×
General Source Logs About	Log path C:\Program Files (x86)\Devolutions\Devolu Show logs Send Error Report
	Save Cancel

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*.

÷	Web Source Selection
	Baba Hub
	DPS

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*.



Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub Master key and click Next.



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.



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*.

KWeb Source Selection	Authentication	
දීද	Devol Passw	utions ord Hub
	Devolutio	ns
	Log in to conti	nue
🛎 Username		
A Password		
	Continue	
Forgot Password		Create Account
English Sessions	🔁 Login 🗘 Set	Security, Legal & Privacy

Devolutions Password Hub Credentials

4. Enter your Devolutions Password Hub Master key and click *Next*.



Devolutions Password Hub Master Key

DEVOLUTIONS LAUNCHER MENU



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

E Devolutions Password Server ⊠ (Cloud Zone > RDM 🕨 🔒 🥒 💌 ъ ١ 👻 📕 Coffre (Windjammer IT) Jump Host Server Coffre (Windjammer IT)
 Credentalis
 Credentalis
 Domain Tools
 B Cloud Zone
 R D Gateway
 R DM Jump Server
 Jump Host Server \$ **•** ATTA OVERVEW ୍ 10.10.0.18 VSRV-JUMP ☆ 192,168,7,18 RDP via Jump Server Ē SSH via Jump Server **⊙**₿ > 🔋 SSH Tur 昆 In-house
 Internal Tool TAGS Jump > [Third Party t Tools

Click the play button bor 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.

E Pevolutions Password Hub	W	Windjammer IT 🗸 🗸	4 🔞
🛞 Vault	Filter 🔇	Microsoft RDP RDP (Microsoft Remote Desktop)	A 1 :
Private vault	CREDENTIALS		
O Search	Global Administrator	Username	G-1
•	Schema Administrator	ben@telemark.loc	-1
	Windjammer20 GQWWNXG25C	Computer VTELESRV-DC1.telemark.loc	
	Windjammer21 W44R319DAG	Descured	
	CREDIT CARD	Massword	Ē: 📀
	T Card 1254-5689-****		
	DOCUMENT	Created On	
	Miagram_DPS-Demo	2019-07-20 02:25:33	
	RDP (MICROSOFT REMOTE DESKTOP)		
Micr VTELE	Microsoft RDP VTELESRV-DC1.telemark.loc:-1	Attachments Access and view files attach to this credentials	>
E Reports	SOFTWARE LICENSE	- Documentation	
Administration	MSOffice MSOffice	Store information regarding entries using the built-in markdown editor	>
Tools	SSH PORT FORWARD	- Logs	
1.9.0.79	SSH Bastion server	^{IEJ} View entry log	>

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.

Close
Close all
Close all but this
Send Ctrl-Alt-Delete
Full screen
Reconnect
Zoom In
Zoom Out
Zoom 1:1

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 be 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 IX

9 Support/Resources

9.1 FAQ (Frequently Asked Questions)

WHAT IS DEVOLUTIONS PASSWORD SERVER?

Devolutions Password Server is a specialized data source for our various client applications of the **Remote Desktop Manager** platform.

WHY BUY DEVOLUTIONS PASSWORD 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 PASSWORD SERVER?

Devolutions Password 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 Password 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 PASSWORD SERVER?

Yes - <u>Request a trial</u>

DOES DEVOLUTIONS PASSWORD SERVER INCLUDE A CLIENT LICENSE OF REMOTE DESKTOP MANAGER?

Devolutions Password Server does not include any client licenses.

IS DEVOLUTIONS PASSWORD SERVER SUBSCRIPTION BASED?

Yes, Devolutions Password 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 PASSWORD SERVER? IS MY DATA STILL ACCESSIBLE?

Yes, once your Devolutions Password Server subscription is expired you can still access the data using one of our applications. However the Devolutions Password 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 PASSWORD SERVER?

Yes, the underlying SQL server database structure for the SQL Server data source is a subset of the Devolutions Password Server database structure. When installing/configuring the Devolutions Password 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 PASSWORD SERVER DOWN TO SQL SERVER DATA SOURCE?

Yes, since the database for Devolutions Password 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 Password Server features will be accessible when using the SQL Server data source, you will need to review all security permissions.

9.2 Follow Us

OVERVIEW

Get the hottest information about our products - tips and tricks, case studies and new release announcements!

This is not a marketing newsletter. We focus on the issues that matter to you, whether you're looking for up-to-the-minute software tutorials, additional outside resources, or a peek at how others are using our products.



E	<u>Twitter</u>
You Tube	<u>YouTube</u>
B	<u>Blog</u>
γ	<u>Forum</u>
C	<u>Spiceworks</u>
Ś	<u>Reddit</u>
0	<u>Instagram</u>

9.3 Previous Versions

DESCRIPTION

Here are the links to the pdf manuals of past releases.

Devolutions Password Server 4.6

Devolutions Password Server 4.5

Devolutions Password Server 4.0

Devolutions Password Server 3.2

Devolutions Password Server 3.0

Devolutions Password Server 2.5

9.4 Technical Support

Hours Monday to Friday 7:30 a.m. to 6:00 p.m. EST

Langu English-Français-Deutsch age:

Email: ticket@devolutions.net

Forum https://forum.devolutions.net/

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 <u>Support Policy</u> for more information.



9.5 Knowledge Base

9.5.1 Azure portal configuration guide for Office365 authentication

DESCRIPTION



Microsoft Azure AD subscription is required to configure Office365 authentication in Devolutions Password Server.

The following topic contains the procedure to configure Azure and Devolutions Password Server properly to use Office365 authentication.

REQUIREMENTS

- Devolutions Password Server Scheduler installed and running.
- Microsoft Azure AD subscription.
- An Azure Public client (mobile & desktop) Application for the Remote Desktop Manager Native application.
- 2 Azure AD Web Application. One for the Devolutions Password Server Web application and the other one for the **Users** and **Roles** Cache application.

CREATION OF AZURE AD APPLICATIONS AND DEVOLUTIONS PASSWORD SERVER OFFICE365 CONFIGURATION.

- 1. Log in to your Microsoft Azure Portal using administrator credentials at https://portal.azure.com.
- 2. To simplify the configuration steps and to easily copy and paste all the required parameters, please have side by side the Azure Portal and the Devolutions Password Server Console opened.
- 3. Once logged in, go to *Azure Active Directory Properties*.
 - 3.1. Click on the Copy to clipboard button beside the Directory ID property.

Home > Devolutions Inc Properties		
Devolutions Inc Properties Azure Active Directory		
,⊃ Search (Ctrl+/) ≪	🕞 Save 🗙 Discard	
App registrations		
App registrations (Legacy)	Directory properties	
Identity Governance	* Name	
Application proxy	Devolutions Inc.	
🔓 Licenses	Country or region Canada	
🚸 Azure AD Connect	Location	
🕫 Custom domain names	United States datacenters	
Ø Mobility (MDM and MAM)	Notification language	
📍 Password reset		
Company branding	Directory ID	
User settings		
11 Properties	n	

Azure AD Directory ID

3.2. Paste this value in the **Tenant ID** field of the Devolutions Password Server **Office365** tab.

Devolutions Password Server Console - Password Server Settings –						\times
Passwore	d Server Settings					
General Database	Office365 Parameters					
Authentication	Tenant ID	4c	5a			
Domain Office365	Native application (RDM)					
IIS Advanced	Client ID	4a	d1			
	Resource ID	0000002-0000-0	000-c000-000000000000			
	Redirect URI	rdm://dps				
	Web application					

Office365 Tenant ID

4. Go to Azure Active Directory - App registrations.



Microsoft Azure Portal

5. DEVOLUTIONS PASSWORD SERVER NATIVE APPLICATION (RDM)

5.1. Create the application using **New registration** button.

Home > Devolutions Inc A	pp registration	ns		
Devolutions Inc Ap Azure Active Directory	op registra	tions		
	«	+ New registration	Endpoints	🗙 Troubleshooting
-		Welcome to the n	ew.and.improved.A	nn registrations (now Ge
	Azure	e AD - App registratio	ons	

- 5.2. Choose a significant name for the application. This name will not be used outside of Azure Portal.
- 5.3. Set which **Supported account types** that will be allowed to connect. Usually selecting **Accounts in this organizational directory only** is more than enough for your Azure AD authentication.
- 5.4. Set the **Redirect URI** to **Public client (mobile & desktop)** and set a valid URI. This value must respect the Azure URI format and must be the same in the Devolutions Password Server Office365 settings.

Home > Devolutions Inc App registrations > Register an application
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Windjammer RDM
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Devolutions Inc.)
Accounts in any organizational directory
Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is
optional and it can be changed later, but a value is required for most authentication scenarios.
Public client (mobile & desktop) 🗸 rdm://dps
By proceeding, you agree to the Microsoft Platform Policies 🔀
Register

Azure Client (RDM) application parameters

5.5. Copy this URI and click on the **Register** button to complete the application registration.

5.6. Paste the URI in the **Redirect URI** field of the **Native application (RDM)** section of the Devolutions Password Server **Office365** tab.

Devolutions Passwo	ord Server Console - Password S	Server Settings		_	×
Password	d Server Settings				
General Database	Office365 Parameters				
Authentication	Tenant ID	4c	5a		
Domain		L			
Office365	Native application (RDM)				
IIS	Client ID	4a	d1		
Advanced	Resource ID	0000002-0000-0000-c000-000000000	000		
	Redirect URI	rdm://dps			
	Web application				

Native Application (RDM) - Redirect URI

5.7. Click on the **Copy to clipboard** button beside the **Application (client) ID** of the Azure client (RDM) application.

Home > Devolutions Inc App registrati	ons > Windjammer RDM	
Windjammer RDM		
	🛅 Delete 🌐 Endpoints	
Overview	Display name : Windjammer RDM	Copy to clipboard
Ouickstart	Application (client) ID : 4a	d1 🗋
	Directory (tenant) ID : 4c	5a
Manage	Object ID : 42	92
🐱 Branding		

Azure Client (RDM) Application ID

5.8. Paste the Application (client) ID in the Client ID field of the Native application (RDM) section of the Devolutions Password Server Office365 tab.

Devolutions Passwo	ord Server Console - Passwo	rd Server Settings		—	×
Passwore	d Server Settings				
General Database	Office 365 Parameters]
Authentication Domain	Tenant ID	4c	5a		
Office365	Native application (RDM)				
IIS	Client ID	4a	d1		
Advanced	Resource ID	0000002-0000-000	00-c000-000000000000		
	Redirect URI	rdm://dps			
	Web application				

Native Application (RDM) - Client ID

5.9. Select the **Authentication** tab of the Azure client (RDM) application and enable the **ID tokens** under **Advanced settings** section.

Home > Devolutions Inc App registrat	Home > Devolutions Inc App registrations > Windjammer RDM - Authentication					
lindjammer RDM - Aut	hentication					
	Rave X Discard Y Try out the new experience Got feedback?					
Overview	Advanced settings					
🕰 Quickstart	Logout URL 👩 e.g. https://myapp.com/logout					
Manage						
🐖 Branding	Implicit grant					
Authentication	Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.					
📍 Certificates & secrets	To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:					
API permissions	Access tokens					
Expose an API						
Owners						
0 Manifest						

Azure Client (RDM) Application - Authentication

5.10. Select the **API Permissions** tab of the Azure client (RDM) application and click on the **Add a permission** button.

Home > Devolutions Inc App registrat	ions > Windjammer RDM - API permissions			
₋ Windjammer RDM - API	permissions			
	API permissions			
🖶 Overview	Applications are authorized to use APIs by r	equesting permissions. These	permissions show up during the cons	sent process where users are given the opportunity to
📣 Quickstart	grant/deny access.			
Manage	+ Add a permission			
5 Branding	API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Authentication	 Microsoft Graph (1) 			
Certificates & secrets	User.Read	Delegated	Sign in and read user profile	-
→ API permissions	These are the permissions that this applicati able permissions dynamically through code.	ion requests statically. You ma . See best practices for reque	y also request user consent- sting permissions	

Azure Client (RDM) Application - Add a permission

5.11. At the bottom of the permissions list, click on the **Azure Active Directory Graph** button.



Azure Client (RDM) Application - Azure Active Directory Graph

5.12. Click on the **Delegated permissions** button.

Request API permissions	
Azure Active Directory Graph APIs are available via the Microse	oft Graph API. You may want to consider using Microsoft Graph instead.
What type of permissions does your application require?	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.

Azure Client (RDM) Application - Delegated Permissions

5.13. Select **User.Read** under **User** section and click on the **Add permissions** button.

▼ User (1)	
☑ User.Read Sign in and read user profile ●	-
User.Read.All Read all users' full profiles	Yes
User.ReadBasic.All Read all users' basic profiles	-
Add permissions Discard	

Azure Client (RDM) Application - User.Read Permission

5.14. The following screen shows the actual permissions set for the Azure client (RDM) application.

API permissions			
Applications are authorized to use APIs by requ grant/deny access.	esting permissions. These	permissions show up during the consent process	where users are given the opportunity to
+ Add a permission			
API / PERMISSIONS NAME	ТҮРЕ	DESCRIPTION	ADMIN CONSENT REQUIRED
 Azure Active Directory Graph (1) 			
User.Read	Delegated	Sign in and read user profile	
 Microsoft Graph (1) 			
User.Read	Delegated	Sign in and read user profile	-
These are the permissions that this application able permissions dynamically through code. Se	requests statically. You ma e best practices for reque	y also request user consent- sting permissions	

Azure Client (RDM) Application - Permissions

5.15. Select the **Manifest** tab and copy the resource application ID of the Azure client (RDM) application which contains the **00000002** value at the beginning.

h



Azure Client (RDM) Application Manifest - Resource ID

5.16. Paste the resource application ID in the **Resource ID** field of the **Native** application (RDM) section of the Devolutions Password Server Office365 tab.

Devolutions Pass	sword Server Console - Passw	vord Server Settings		—	×
Passwo	ord Server Settings	;			
General Database	Office 365 Parameters				
Authentication Domain	Tenant ID	4c.	5a		
Office365	Native application (RDM)			
IIS Advanced	Client ID	4a	d1		
	Resource ID	0000002-0000-00	00-c000-00000000000		
	Redirect URI	rdm://dps			
	Web application				

Native Application (RDM) - Resource ID

6. DEVOLUTIONS PASSWORD SERVER WEB APPLICATION

6.1. Create the application using the **New registration** button in Azure portal.

Home > Devolutions Inc App registrations			
Devolutions Inc App registrations Azure Active Directory			
	+ New registration	🕀 Endpoints	🗙 Troubleshooting
Welcome to the new and improved App registrations (now Gener			

Azure AD - App registrations

- 6.2. Choose a significant name for the application. This name will not be used outside of Azure Portal.
- 6.3. Set which **Supported account types** that will be allowed to connect. Usually selecting **Accounts in this organizational directory only** is more than enough for your Azure AD authentication.
- 6.4. Set the **Redirect URI** to Web and set a valid URL. This property must be set with the URL to reach your Devolutions Password Server instance with **/login** at the end.
| Home > Devolutions Inc App registrations > Register an application |
|---|
| Register an application |
| |
| * Name |
| The user-facing display name for this application (this can be changed later). |
| Windjammer Web |
| |
| Supported account types |
| Who can use this application or access this API? |
| Accounts in this organizational directory only (Devolutions Inc.) |
| Accounts in any organizational directory |
| Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com) |
| Help me sheese |
| hep the choose |
| |
| Redirect ORI (optional) |
| We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios. |
| Web V https://windsrv-dvls.windjammer.loc/dps/login V |
| |
| By proceeding, you agree to the Microsoft Platform Policies 12 |
| |
| Register |

Azure Web Application Paramaters

- 6.5. Then, click on the **Register** button to create the application.
- 6.6. Click on the Copy to clipboard button of the Application (client) ID.

Home > Devolutions Inc App registrations > Windjammer Web Windjammer Web					
	🛅 Delete 🛛 🜐 Endpoints				
Overview	Display name : Windjammer Web	Copy to clipboard			
Ouickstart	Application (client) ID : b2	31 🖒			
Quickstart	Directory (tenant) ID : 4c	5a			
Manage	Object ID : 72	0			

Azure Web Application ID

6.7. Paste the **Application (client) ID** in the **Client ID** field of the **Web application** section of the Devolutions Password Server **Office365** tab.

□ Devolutions Password Server Console - Password Server Settings - □ ×						
Password	d Server Settings					
General	Office365 Parameters					
Database Authentication Domain	Tenant ID	4c	5a			
Office365	Native application (RDM)					
IIS	Client ID	4a	ld1			
Auvanceu	Resource ID	00000002-0000-0000-c000-00000000	0000			
	Redirect URI	rdm://dps				
	Web application					
	Client ID	b2	31			
Users and Roles Cache						

Web Application - Client ID

6.8. Select the **Authentication** tab of the Azure Web application and enable the **ID tokens** under **Advanced settings** section.

Home > Devolutions Inc App registrations > Windjammer Web - Authentication					
Windjammer Web - Auth	nentication				
	Example Save X Discard Y Try out the new experience Got feedback?				
Overview	Advanced settings				
📣 Quickstart	Logout URL 👩 e.g. https://myapp.com/logout				
Manage					
🚾 Branding	Implicit grant				
	Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.				
💡 Certificates & secrets	To enable the implicit grant flow select the tokens you would like to be issued by the authorization endpoint:				
API permissions	Access tokens				
🚳 Expose an API					
Owners	V ID tokens				

Azure Web Application - Authentication

7. DEVOLUTIONS PASSWORD SERVER USERS AND ROLES CACHE APPLICATION

7.1. Create the application using **New application registration** button.

Home > Devolutions Inc App regis	trations		
Devolutions Inc App regination	strations		
	 New registration 	Endpoints	🗙 Troubleshooting 🛛
	Welcome to the ne	w and improved A	nn registrations (now Gener

Azure AD - App registrations

- 7.2. Choose a significant name for the application This name will not be used outside of Azure Portal.
- 7.3. Set which **Supported account types** that will be allowed to connect. Usually selecting **Accounts in this organizational directory only** is more than enough for your Azure AD authentication.
- 7.4. Set the Redirect URI to Web and set a valid URL.

Home > Devolutions Inc App regist	rations > Register an application
Register an application	
* Name	
The user-facing display name for this	application (this can be changed later).
Windjammer Sync	✓
Supported account types	
Who can use this application or acces	s this API?
• Accounts in this organizational dir	ectory only (Devolutions Inc.)
O Accounts in any organizational dir	ectory
O Accounts in any organizational dir	ectory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
Help me choose	
Redirect URI (optional)	
We'll return the authentication respons	se to this URI after successfully authenticating the user. Providing this now is
optional and it can be changed later, l	but a value is required for most authentication scenarios.
Web 🗸	https://vwindsrv-dvls.windjammer.loc/dps
By proceeding, you agree to the Micro	osoft Platform Policies 🛛
Register	

Azure Sync Application Paramaters

- 7.5. Copy this URI and click on the **Register** button to create the application.
- 7.6. Paste the URI in the **Redirect URI** field of the **Users and Roles Cache** section of the Devolutions Password Server **Office365** tab.

Devolutions Password Server Console - Password Server Settings –							
Passwo	ord Server Settings						
General	Office 365 Parameters						
Database Authentication Domain	Tenant ID	4c	5a				
Office365	Native application (RDM)						
IIS Advanced	Client ID	4a	d1				
Advanced	Resource ID	0000002-0000-000	00-c000-00000000000				
	Redirect URI	rdm://dps					
	Web application						
	Client ID	b2	31				
	Users and Roles Cache						
	Client ID	ac	с9				
Redirect URI https://vwindsrv-dvls.windjammer.loc/dps							
	Secret key	•••••					

Users and Roles Cache - Redirect URI

7.7. Click on the Copy to clipboard button of the Application (client) ID.

Home > Devolutions Inc App registration	ons 🗧 Windjammer Sync	
Windjammer Sync		
,⊅ Search (Ctrl+/) ≪	🛅 Delete 🛛 🜐 Endpoints	
Overview	Display name : Windjammer Sync	Copy to clipboard
🗳 Quickstart	Application (client) ID : ac	с9 Ц <u>ъ</u> i5a
Manage	Object ID : ee	2e9
5 Branding		

Azure Sync Application - Application (Client) ID

7.8. Paste the **Application (client) ID** in the **Client ID** field of the **Users and Roles Cache** section of the Devolutions Password Server **Office365** tab.

Devolutions Password Server Console - Password Server Settings – □							
Passwo	ord Server Settings						
General	Office365 Parameters						
Database							
Authentication	Tenant ID	4c	5a				
Office365	Native application (RDM)						
IIS Advanced	Client ID	4a	d1				
Advanced	Resource ID	0000002-0000-0000	-c000-00000000000				
	Redirect URI	rdm://dps					
	Web application						
	Client ID	b2	31				
	Users and Roles Cache						
	Client ID	ad	c9				
	Redirect URI	https://vwindsrv-dvls	windjammer.loc/dps				
	Secret key	•••••	•••••				

Users and Roles Cache - Client ID

- 7.9. In the Azure Sync application, select **Certificates & Secrets** to create a new client secret.
- 7.10. Click on the **+ New client secret** button, set a description and when this client secret key will expire. Then click on the **Add** button.

Home > Devolutions Inc App registrat	ions > Windjammer Sync - Certificates & secrets
💡 Windjammer Sync - Cert	ificates & secrets
	Add a client secret
Overview	Description
📣 Quickstart	Windjammer Sync
Manage	Expires
🐖 Branding	🚫 In 2 years
Authentication	Never
📍 Certificates & secrets	
API permissions	Add Cancel
Expose an API	
n Owners	Client secrets
10 Manifest	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
Support + Troubleshooting	+ New client secret
✗ Troubleshooting	DESCRIPTION EXPIRES VALUE
New support request	No client secrets have been created for this application.

Azure Sync Application - Client secret Creation

7.11. Click on the **Copy to clipboard** button of the **Client secret**. Be sure to save the **Client secret** in a safe place as once you will switch to another page of the Azure portal, the copy button will no longer be available.

Client secrets				
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.				
+ New client secret				
DESCRIPTION	EXPIRES	VALUE		
Windjammer Sync	12/31/2299	J/	v+ 🗈	ā

Azure Sync Application - Client secret

7.12. Paste the **Client secret** in the **Secret key** field of the **Users and Roles Cache** section of the Devolutions Password Server **Office365** tab.

Devolutions Password Server Console - Password Server Settings						
Passwor	d Server Settings					
General	Office 365 Parameters					
Database						
Authentication	Tenant ID	4c 5a				
Domain	Native analization (DDM)					
Office365	Native application (RDP)					
IIS	Client ID	4a d1				
Advanced	Resource ID	0000002-0000-0000-c000-000000000000				
	De dise st UDT					
	Redirect URI	rdm://dps				
	Web application					
	Client ID	b2 31				
	Users and Roles Cache					
	Client ID	ad c9				
	Redirect URI	https://vwindsrv-dvls.windjammer.loc/dps				
	Secret key	•••••				
	Users and Roles Cache Client ID Redirect URI Secret key	ac c9 https://vwindsrv-dvls.windjammer.loc/dps				

Users and Roles Cache - Secret key

7.13. the Azure Sync application, select **API permissions** or click on the **View API Permissions** button to set the proper permissions on the Sync application.



Azure Sync Application Permissions

7.14. Click on the + Add a permissions button.



Azure Sync Application API Permissions

7.15. Select Microsoft Graph.



Azure Sync Application Request Permissions - Microsoft Graph

7.16. Select Application permissions.

Request API permissions	
 ✓ All APIs Microsoft Graph https://graph.microsoft.com/ Docs What type of permissions does your application require? 	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.

Azure Sync Application - Application Permissions

7.17. Select **Group.Read.All** permission under section Group and **User.Read.All** permission under User section. Then click on the **Add permissions** button.

▼ Group	(1)	
V	Group.Read.All Read all groups 🕤	Yes
	Group.ReadWrite.All Read and write all groups 💿	Yes

Azure Sync Application - Group Permission

▼ User (1)		
User.Export.All Export user's data 💿	Yes	
User.Invite.All Invite guest users to the organization 💿	Yes	
User.Read.All Read all users' full profiles 💿	Yes	
User.ReadWrite.All Read and write all users' full profiles 🕕	Yes	
Add permissions Discard		

Azure Sync Application - User Permission

7.18. Select the **User.Read Delegated** permission and click on the **Remove permission** button as this permission isn't required for the Sync application.

Home > Devolutions Inc App registrations > Windjammer Sync - API permissions					User.Read ×
ے۔ Windjammer Sync - API permissions					Microsoft Graph
«					Remove permission
Ja search (Ctn+/)	API permissions				https://graph.microsoft.com/User.Read []h
K Overview	Applications are authorized to use APIs by requesti	ng permissions. These	e permissions show up during the consent process when	e users are	
📣 Quickstart	grant/deny access.				No
Manage	+ Add a permission				
Branding	API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMI	Admin consent display name Sign in and read user profile
Authentication	 Microsoft Graph (3) 				
📍 Certificates & secrets	Group.Read.All	Application	Read all groups	Yes	Admin consent description Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also
API permissions	User.Read	Delegated	Sign in and read user profile	-	allows the app to read basic company information of signed-in users.
Expose an API	User.Read.All	Application	Read all users' full profiles	Yes	User consent display name
Owners	These are the permissions that this application requ	uests statically. You ma	av also request user consent-		
Manifest	able permissions dynamically through code. See b	est practices for requ	esting permissions		User consent description Allows you to give into the approxitibly your organizational account and let the approach your profile. It
Support + Troubleshooting					allows you to sign in to the app with your organizational account and let the app read your prome. It also allows the app to read basic company information.
★ Troubleshooting	Grant consent				Docs 🗹
New support request	To consent to permissions that require admin conse this directory.	ent, please sign in witl	h an account that is an administrator for		
	Grant admin consent for Devolutions Inc.				

Azure Sync Application - Remove Permission

8. This is how the Devolutions Password Server Office365 tab settings should look like.

Devolutions Passwe	ord Server Console - Password	Server Settings	_	
Passwor	d Server Settings			
General	Office365 Parameters			
Authentication	Tenant ID	4c 5a		
Office365	Native application (RDM)			
IIS	Client ID	4a vd1		
Advanced	Resource ID	00000003-0000-0000-c000-00000000000		
	Redirect URI	rdm://dps		
	Web application			
	Client ID	b2 31		
	Users and Roles Cache			
	Client ID	ad c9		
	Redirect URI	https://vwindsrv-dvls.windjammer.loc/dps		
	Secret key	•••••	••	
	Automatic User Creation			
	Auto create Office 365 users			
	Default Vault	Create read-only user	*	
	Office 365 Users And Roles Cache			
	Update users and groups data ev	ery: 0 + Hours 30 +	minutes	
	Test Connection			
	Search property	1	Save	Cancel

Devolutions Password Server Office 365 Tab settings

9. Finally, enable the **Use Office365** authentication option in *File - Data Sources* in Remote Desktop Manager or use the **Office 365 Log In** button on the web interface.

📮 Remot	📮 Remote Desktop Manager - Devolutions Password Server 🛛 🚽 🔿			×				
	Devol	utions P	asswor	d Serve	r			
General	Settings	Private Vault	Advanced					
	lame lost Isername	Devolu http:// Use Alw user 1@	tions Password windsrv-dvls/o Windows auth Office365 auth ays prompt for	l Server dps entication hentication credentials .com	~			
	855W010	Alw	ays ask passwo	ord		Test (Connectio	n
ID 515	CE1AA-B383	3-43FF-AD45-E8	3CCAC4022A			ОК	Can	icel

Remote Desktop Manager Data Source Configuration

Devolutions Password Server	-
Log in to your account	
Office 365 Log In	
OR	
Username	*
Password	*
Log In	

Devolutions Password Server Login page

9.5.2 Backup and restore Devolutions Password Server

DESCRIPTION

The following topic describes the requirements and the step to properly configure the Devolutions Password Server Backup Scheduler and instructions on how to restore your Devolutions Password Server instance succeeding a disaster.



Check the backup of the SQL database and the web application folder integrity by restoring them in a staging environment.

BACKUP CONFIGURATION

1. Install the **DevolutionsSchedulerService** with the **Install Scheduler** button of the Devolutions Password Server Console if it is not already installed. For more information please see <u>Devolutions Password Server Console</u>.



2. Create a domain service account that will be use to run the service.

DevolutionsSchedulerSe	rvice (dvlsorion) Properties (Local Comput	×
General Log On Reco	very Dependencies	
Log on as:		
O Local System accourt	it	
Allow service to in	teract with desktop	
This account:	VaultScheduler@orion.loc Browse	
Password:	•••••	
Confirm password:	•••••	
	OK Cancel Apply	

DevolutionsSchedulerService - Log On properties

3. This service account must have proper permission on the destinations folder(s) to create files and needs at least the db_datareader and db_backupoperator rights on the SQL database.

Login Properties - ORION\Va	ultScheduler			_		×
Select a page	🖵 Script 🔻 🄇	Help				
Server Roles User Mapping	Users mapped	to this login:				
Securables	Map Da	tabase	User	Default Schema		
📕 Status	🗹 dv	lsorion	ORION\VaultScheduler	dbo		
	ma	ster				
	mo	del				
	ms	db				_
	ter	npdb				
Connection						
Comine Co	Guest acco	ount enabled for: d	lvlsorion			
Server: MINTAKA\SQL2016	Database role	membership for: d	vlsorion			
Connection:	db access	admin				
sa	db_backup	operator				
View connection properties	✓ db_datarea	ider ter				
	db_ddladm	in				
	db_denyda	tareader				
Progress	db_denyda	tawriter				
	db_security	vadmin				
Ready	public					
				ОК	Ca	ncel

Service account - SQL Permissions

- 4. Create a network folder, it can be one for the database backup and one for the web application backup, that both the server which hosted the Devolutions Password Server instance and the SQL Server will have access to.
- 5. Configure the options in the **Backup Manager**. For more information please see <u>Backup Manager</u>.
- 6. In the following sample:

- The database backup is **enabled** and will be saved in folder **TeamShare\BackupDVLS\DB** on DC machine.

- The web backup is **enabled** and will be saved in folder **TeamShare\BackupDVLS\Web** on DC machine.

- The administrators will be notified on backup failed
- The scheduled backup has been started on August 1st, 2018 at 1:00 AM.
- The scheduler will repeat the backup process every day.

8		_		×
Backup configuration				
Database Advanced				
Database Configuration			Save	
Enable database backup			Cancel	
Backup database file path	\\DC\TeamShare\BackupDVLS\DB		Backup No	w
Web Configuration				
Enable web backup				
Backup database file path	\\DC\TeamShare\BackupDVLS\Web			
Schedule				
Notify Administrator on backup fa	iled 🗹			
Backup start time 2018-08-01	I:00:00 AM ►			
Repeat every Days 1	Hours 0 🗘 Minutes 0			

Backup Scheduler Configuration - Database Tab

RESTORE STEPS

The following instructions explain how to restore the Devolutions Password Server environment. The first part explains the restore process on an existing installation and the second part details the steps to restore Devolutions Password Server on new machines.

Ensure that all prerequisites are installed on the machine where the Devolutions Password Server instance is hosted. For more information please see <u>Installing Web Roles prerequisites</u>.

?

If the Devolutions Password Server deployment is hosted in a **Load Balancing** or **High Availability** topology, please see <u>Manage</u> <u>Encryption Keys</u>.



Be sure that the database and the web application match before launching the restore process or this could lead to unwanted behavior.

- 1. If the restore process goal is to overwrite the current installation :
 - a. Ensure that the instance users have the offline mode enabled and they are not making any modifications.
 - b. Ensure that the **DevolutionsSchedulerService** service is not running.

DevolutionsSche	dulerService (dvlsorion) Properties (Local Comput $ imes$
General Log On	Recovery Dependencies
Service name:	DevolutionsSchedulerServicedvlsorion
Display name:	DevolutionsSchedulerService (dvlsorion)
Description:	Devolutions Server Scheduler Service
Path to executat "C:\inetpub\www	ole: wroot\dvlsorion\bin\Devolutions.Server.Service.exe''
Startup type:	Automatic ~
Service status:	Stopped
Start	Stop Pause Resume
You can specify from here.	the start parameters that apply when you start the service
Start parameters	:
	OK Cancel Apply

DevolutionsSchedulerService

- c. Restore the SQL database.
- d. Overwrite the web application folder with the content of the web application .zip file.
- e. Start the **DevolutionsSchedulerService** service and ensure that the **Startup** type is set to **Automatic**.

DevolutionsSchedulerService (dvlsorion) Properties (Local Comput $ imes$
General Log On Recovery Dependencies
Service name: DevolutionsSchedulerServicedvlsorion
Display name: DevolutionsSchedulerService (dvlsorion)
Description: Devolutions Server Scheduler Service
Path to executable: "C:\inetpub\wwwroot\dvlsorion\bin\Devolutions.Server.Service.exe"
Startup type: Automatic ~
Service status: Running
Start Stop Pause Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK Cancel Apply

DevolutionsSchedulerService

- f. Reconfigure the **Backup Scheduler** feature.
- 2. If the goal is to restore Devolutions Password Server and the SQL database on new servers :
 - a. Restore the SQL database on the new server.
 - b. Fix every SQL login account that have been used to connect on the database from
 - c. Follow instructions of <u>Create Devolutions Password Server instance</u> topic.
 - d. **Overwrite** the web application folder with the content of the web application .zip file.
 - e. Reconfigure the Backup Scheduler feature.

9.5.3 Command Line Interface

A Command Line Interface (CLI) is a Companion Tool which allows DPS users to access credentials with the command line.

Listed below are the available command line:

CONFIG

Parameters:

-v --vault

-s --server

The address of the server to connect to.

If you call config without parameters, it will return the current settings.

Options:

-j --json

The command output will be formatted in JSON format.

Examples:

DPS> config

Server: http://localhost/dvls/api

Vault: 000000-0000-0000-0000-000000000000

DPS> config --server http://localhost/dvls/api

DPS> config -v 12345678

```
DPS> config --json
```

GET

Returns the credentials of an entry based on its id.

Parameters:

The entry's id can be found in its advance property or in the last part of its URL.



Advanced Credentials - Username / Password

Options:

-j --json

The command output will be formatted in JSON format.

-d --domain

Only returns the domain.

-u --username Only returns the username.

-p --password

Only returns the password.

Examples:

DPS> get 4574725f-0d24-4cbc-a116-a5270179e251

domain: dddd

username: asdf

password: 12345

DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 --json

```
{
    "domain": "dddd",
    "username": "asdf",
    "password": "12345"
}
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 -u
asdf
```

DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 -p

12345

```
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251
    domain: ddd
    username: asdf
    password: 12345
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 --json
{
    "domain": "dddd",
    "username": "asdf",
    "password": "12345"
}
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 --domain --json
{"domain":"dddd"}
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 --username --json
{"username":"asdf"}
DPS> get 4574725f-0d24-4cbc-a116-a5270179e251 --password --json
{"password":"12345"}
DPS>
```

Get Example

LOGIN

Parameters:

First parameter: the username (the key, if the user is of the type application)

Second parameter: the password (the secret, if the user is of the type application)



Application User

The user/application must have the right to use the CLI

Edit user		2 ×
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

Applications Edit User CLI

Options:

-j --json

The command output will be formatted in JSON format.

Examples:

DPS> login dsavard 12345



Login Example

LOGOUT

Logout the current user.

DPS> logout Logout Successful

Logout Example

SET

Update the credentials of an entry.

Parameters:

The entry's id can be found in its advance property or in the last part of its URL.

🔒 Pa	assword	Server - Connections X	+		-		×
← →	> C	nnections/0000000	0-0000-0000-0000-00000000000000/9bb24938-6787-4da8-b9ca-a51f342792a3	, Q	☆) e	:
≡	B R	evolutions assword Server	Vault 🗸				
©	-	Credentials - Use	rname / Password	• ×		E	
⊕ o, ☆	Ţ	GENERAL MORE SECURITY USER INTERFACE EMAIL NOTIFICATIONS ADVANCED	Database ID D806DF94-EC4C-4448-8190-96122C6493F5 Session ID 9bb24938-6787-4da8-b9ca-a51f342792a3				
			Update	Cancel			
2019.2.2.0		Customer issues Entries				6	

Advanced Credentials - Username / Password

Options:

-j --json

The command output will be formatted in JSON format.

-d --domain new-value

Update the domain.

-u --username new-value

Update the username.

-p --password new-value

Update the password.

Examples:

DPS> set 4574725f-0d24-4cbc-a116-a5270179e251 --domain newdomain

Entry has been successfully updated



Set Example

9.5.4 Configure Client Data Source

CREATE DEVOLUTIONS PASSWORD SERVER DATA SOURCE

1. Select File - Data Sources.



File - Data Sources

2. New Data Source.

🖪 Remote	Remote Desktop Manager ×					
+ 🗲	X 🕏	5				
General	Settings	Private Vault	Upgrade	VPN	Advanced	

Data Source Configuration Dialog

3. Select the **Devolutions Password Server** data source.

🔲 Remote Desktop Manager -	Add New Data Source		×
😂 Add New Da	ta Source		
All	Individual Devolutions Online Drive Free Google Drive Free Xml Free Team	Dropbox Free SQLite Free	^
	Microsoft Access Enterprise MariaDB Enterprise Devolutions Online Database Enterprise Amazon S3 Enterprise Microsoft SQL Server Enterprise Web Enterprise	FTP Enterprise MySQL Enterprise Devolutions Password Server Enterprise SFTP Enterprise Microsoft SQL Azure Enterprise WebDav Free	*
		ОК	Cancel

Add New Data Source Dialog

4. Specify settings.

If you specify % USERDOMAIN% \% USERNAME% in the user text area, the value of the corresponding environment variables will be used.

Remote Desktop Manager	_		×
Devolutions Server			
Connection Settings Advanced			
Name Devolutions Server Server http://localhost/DVLS		~	3
Username david@windiammer.loc		-	V
Password Always ask password			
<u>Test Connection</u>			
ID 76F31534-7E27-43D9-B578-E76AA915A924	ОК	Car	cel

Data Source Configuration

NOTES

If the server is configured to only allow SSL, ensure you specify the protocol by using https:// as the protocol.

9.5.5 Configure Devolutions Password Server to be always available

DESCRIPTION

To prevent that the Devolutions Password Server web application will recycle periodically and to be on idle mode, please follow these instructions.

 Open IIS Manager and expand the Tree View and select Application Pools. In the Application Pools list, select your web application and click on Advanced Settings in the Actions panel on the right. Then, change the Start Mode option to the value AlwaysRunning.



IIS Manager Advanced Settings

Still in the Advanced Settings, set the Idle Time-Out (minutes) option to the value 0. When this value is set to a value different to zero, on the first connection to the web site after an idle period, the application pool needs to create a new process, loads all needed frameworks. These operations can be very slow.

⊿	СРО		^
	Limit (percent)	0	Г
	Limit Action	NoAction	
	Limit Interval (minutes)	5	
	Processor Affinity Enabled	False	
	Processor Affinity Mask	4294967295	
	Processor Affinity Mask (64-bit c	4294967295	=
⊿	Process Model		
⊳	Generate Process Model Event L		
	Identity	windjammer\dbrunner2	
	Idle Time-out (minutes)	0	
	Idle Time-out Action	Terminate	
	Load User Profile	False	
	Maximum Worker Processes	1	
	Ping Enabled	True	
	Ping Maximum Response Time	90	
	Ping Period (seconds)	30	
	Shutdown Time Limit (seconds)	90	
	Startup Time Limit (seconds)	90	~
l d [id idl	e Time-out (minutes) leTimeout] Amount of time (in m e before it shuts down. A worker p quests and no new requests are red	inutes) a worker process will remain rocess is idle if it is not processing reived.	

Application Pool Advanced Settings Dialog

3. Finally, set the **Regular Time Interval (minutes)** option to the value **0**. This will prevent the application pool to recycle periodically.

	Advance	ed Settings ?	x			
	Executable		^			
	Executable Parameters					
⊿	Rapid-Fail Protection					
	"Service Unavailable" Response	HttpLevel				
	Enabled	True				
	Failure Interval (minutes)	5				
	Maximum Failures	5				
	Shutdown Executable					
	Shutdown Executable Parameter					
⊿	Recycling					
	Disable Overlapped Recycle	False				
	Disable Recycling for Configurat	False	Н			
⊳	Generate Recycle Event Log Entr					
_	Private Memory Limit (KB)	0				
	Regular Time Interval (minutes)	0	≡			
1	Request Limit	0				
⊳	Specific Times	TimeSpan[] Array				
	Virtual Memory Limit (KB)	0				
			\sim			
Regular Time Interval (minutes) [time] Period of time (in minutes) after which an application pool will recycle. A value of 0 means the application pool does not recycle on a regular interval.						
		OK Cancel				

Application Pool Advanced Settings Dialog

9.5.6 Configure Devolutions Password Server to use integrated security

DESCRIPTION

In order for integrated security to be used to connect to the database, you must set the **Application pool** to use a domain account to run under.

STEPS

To make these instructions simpler, we will name the domain account **RDMRunner**, please adapt to your requirements.

- Create the VaultRunner account in the domain;
- Grant access to the <u>SQL Server instance</u> to VaultRunner;
- Grant access to the database to VaultRunner;
- In IIS Manager, expand the Application pool section and locate the application pool used by your Devolutions Password Server site. By default it has the same name as the name of the web application;
- In the Advanced Settings, edit the Identity setting to set the VaultRunner account.



9.5.6.1 How to Grant access to SQL Server instance

DESCRIPTION

In order to use **Integrated Security** you will need to grant access and specific permissions to the domain account used to connect to the SQL Server Instance.

STEPS

To make these instructions simpler, we will name the domain account **VaultRunner**, please adapt to your requirements.

1. Using **Microsoft SQL Server Management Studio**, right-click on the **Security** branch and select **New - Login**.



MSSQL

2. In the dialog, click on **Search**.

8	Login -	New		- 🗆 🗙
Select a page	🔄 Script 🔻 🛐 Help			
General Server Roles User Mapping Securables Status	Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password policy Enforce password expiral			Search
	 Mapped to certificate 	ford at next login	v	
	O Mapped to asymmetric key		~	
Connection	Map to Credential		~	Add
Server: vdev33\SQL2014 Connection: VDEV33\Devolutions <u>View connection properties</u>	Mapped Credentials	Credential	Provider	
Progress				Remove
Ready	Default database: Default language:	master <default></default>	~	
			ОК	Cancel

Login - New

3. Change the location to your domain and then select the **VaultRunner** user account.

Select User, Service Account, or (Group
Select this object type: User or Built-in security principal	Object Types
From this location:	
downhill.loc	Locations
Enter the object name to select (<u>examples</u>):	
rdmrunner (rdmrunner@downhill.loc)	Check Names
Advanced	OK Cancel

Select User or Group

4. In the **User Mapping** Section, find your database and check the **Map** checkbox.

8	Login -	New	- 🗆 🗙	
Select a page General Server Roles User Mapping Securables Status	Users mapped to this login: Map Database master model	User	Default Schema	
_	msdb RDM tempdb Guest account enabled for: RE	DM		
Connection Server: vdev33\SQL2014 Connection: VDEV33\Devolutions View connection properties Progress Ready	Database role membership for: RD db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_owner db_securityadmin ✓ public	Μ <u></u>		
			OK Cancel	:

User Mapping
8	Log	in - New	- • ×
Select a page	🔄 Script 🔻 🛐 Help		
Server Roles User Mapping Securables Status	Users mapped to this login: Map Database master model Msdb V RDM tempdb	User	Default Schema
Connection Server: vdev33\SQL2014 Connection: VDEV33\Devolutions VDEV33\Devolutions View connection properties Progress Ready	Database role membership fo db_accessadmin db_backupoperator db_datareader db_datawriter db_ddladmin db_denydatareader db_denydatawriter db_owner db_securityadmin v public	r: RDM	
			OK Cancel

5. In the **Database role membership**, grant the **db_datareader** role and then click **OK** to save the login.

Database Role membership

PERMISSIONS

The permissions needed for the VaultRunner account allow for **ALL** management operations to be performed through the Devolutions Password Server instance.

Some may desire to harden the system. Hardening the system means to **disallow** certain operations from the Devolutions Password Server instance, which would make using a SQL Server data source, **bound to the same database**, necessary for these operations. For instance you could decide to not allow to create users through the instance, but only through a direct SQL connection. Please contact us to discuss these scenarios.



Please note that we are reworking these scripts as there are significant changes to the DB structure in the latest releases. These scripts are mandatory in order to give enough permissions to the VaultRunner service account. Contact our <u>support department</u> for instructions specific to your installed version.

9.5.7 Configure Notifications

DESCRIPTION

The Email Notifications can now be configure at user level in Administration - Users.

STEPS



The <u>Email</u> settings must be configured in the Devolutions Password Server instance in order for notifications to be sent.



The **Allow notification subscription** option must be enable in <u>Administration - Password Server Settings - Scheduler</u> section in order for notifications to be sent.

1. In the **User Management** dialog, select the **Email Notifications** tab and enable the items the user should be notified for in the **Email Notifications** top section.

Devolutions Password Se	rver Console - User Management				×
🔓 User Manag	ement				
General Information Roles Privileges Security Groups Vaults Application Access Settings Email Notifications	Email Notifications Connection opened Data Source Settings changed Entries Vault Roles Security groups Tasks Users Users Users locked out Entry expiring Watched By	30 days	15 days	5 days	
	Username bill@windjammer.loc david@windjammer.loc ellen@downhillpro.xyz erica.poirier@downhillpro.xyz		On Edit	On Delete	
				ОК	Cancel

Connection opened	The user will be notified by email if a connection has been opened.
System Settings (Data Source Settings)	The user will be notified by email if the System Settings has been modified.
Entries	The user will be notified by email if an entry has been added, edited, deleted depending on the selection.
Vault	The user will be notified by email if a Vault has been added, edited, deleted depending on the selection.

Roles	The user will be notified by email if a role has been added, edited, deleted depending on the selection.
Security groups	The user will be notified by email if a security group has been added, edited, deleted depending on the selection.
Tasks	The user will be notified by email if a task has been added, edited, deleted depending on the selection.
Users	The user will be notified by email if a user account has been added, edited, deleted depending on the selection.
Users Locked Out	The user will be notified by email if a user locked his account.
Entry expiring	The user will be notified by email when an entry is almost expired.

 It is possible to set Email Notifications from different Management dialogs. In the User, Vault and Role Management dialog, the lower Email Notifications section will enable notifications for a specific user related to the specific management dialog opened.

In the following screen shot, email notifications on Vaults as been enabled for walter@downhillpros.com user account. So, this user will receive email notifications when Vaults are edited or deleted. If this user wants to get email notifications when a new item is created, this can only be activated from the user properties dialog.

Devolutions Server Console - Repository Management				
p Repositor	y Management			
General Email Notifications	Email Notifications			
Email Nourications	Username	Enabled	Edit	Delete
	jessica.oxley@downhillpros.net			
	walter@downhillpros.com			
	_admin			
			ОК	Cancel

Email Notifications activation from Management Dialogs

9.5.8 Configure SSL

DESCRIPTION

Please perform these steps only after you have configured the Devolutions Password Server instance and that you have indeed connected through a client application. Performing these steps right from the start may add a layer of complexity that may prevent you from succeeding in the initial configuration.

IMPORT CERTIFICATE OR CREATE SELF-SIGNED CERTIFICATE

1. Select the server node in the **Tree View** and double-click the **Server Certificates** feature in the **List View**:



Server certificates

2. Click Import Certificate... in the Actions pane Or Click Create Self-Signed Certificate... in the Actions pane.

internet Information Services (IIS) M	lanager			
COO 9 DEVOLUTIONS18	} •			🕶 🖂 🚱 •
<u>F</u> ile <u>V</u> iew <u>H</u> elp				
Connections	Server Certifica Use this feature to request and m use with Web sites configured for	tes anage certificates that the Web : r SSL.	server can	Actions Import Create Certificate Request Complete Certificate Request
⊿ -@ Sites > -@ Default Web Site @ Site2	Name	Issued To	Issued	Create Domain Certificate Create Self-Signed Certificate Help
				Online Help

Follow the wizard

CREATE A SSL BINDING

1. Select the web site in the **Tree View**.



IIS Tree View

2. Click **Bindings...** in the **Actions** pane. This brings up the bindings editor that lets you create, edit, and delete bindings for your Web site. Click **Add...** to add your new SSL binding to the site.

e Bindi	ngs				<u>? ×</u>
Туре	Host Name	Port	IP Address	Bind	<u>A</u> dd
http		80	*		Edit
					<u>R</u> emove
•					Browse
					Close

Add binding

3. Select **https** in the **Type** drop-down list. Select the self-signed certificate you created in the previous section from the **SSL Certificate** drop-down list and then click **OK**.

dd Site Bi	nding	?
<u>Type</u> :	IP address:	Port:
https	▼ All Unassigned	443
Host name	1	
[
SSL certific	cate:	
Test Certi	ficate	▼ <u>View</u>
-		
Not select	ed	

Define https binding

4. Now you have a new **SSL** binding on your site.



The new binding

CONFIGURE SSL SETTINGS IN IIS

1. Select a Devolutions Password Server application in the **Tree View**.



IIS Tree View

2. Click on SSL Settings.



3. Configure SSL settings if you want your site to require SSL, or to interact in a specific way with client certificates. Click the site node in the **Tree View** to go back to the site's home page. Double-click the **SSL Settings** feature in the middle pane. Select **Require SSL** and click **Apply**.

	Actions	
SSL Settings	Apply	
This page lets you modify the SSL settings for the content of a Web site or application.	Ex Cancel	
Reguire SSL	Online Help	
Require 128-bit SSL		
Client certificates:		
Ignore		
C Accept		
C <u>R</u> equire		



MODIFY THE DEVOLUTIONS PASSWORD SERVER CONFIGURATION

- 1. From the Devolutions Password Server Console, edit the Devolutions Password Server instance.
- 2. Go in the IIS tab and enable the Force https option.

📮 Remote Desktop Mana	iger	_		×
Server S	Settings			
General Database Authentication Domain Two-Factor Security GeoIP Security IIS Email User Interface Logging Features Scheduler Advanced	IIS Settings Website Default Web Site Diagnostic ✓ Force https This option requires that you install an SSL certificate in IIS. Please see IIS documentation on the steps to follow. Manage Certificate ✓ Encrypt web.config file Web application name //dvls Installation folder C:\/inetpub\/wwwroot\/dvls	••••••••••••••••••••••••••••••••••••		
	Si	ave	Can	cel

Forcre https

3. Save the modification with the **Save** button.

CONFIGURE SSL SETTINGS IN THE CLIENT APPLICATIONS

- 1. Edit the Devolutions Password Server data source
- 2. Change the server URL to use the **https://** protocol

9.5.9 Configure Windows Authentication

DESCRIPTION

These steps provide the information to enable the **Windows Authentication** feature in Devolutions Password Server.

STEPS

1. In the **Authentication** tab of the **Server Settings** of the Devolutions Password Server instance, enable the **Enable Windows Authentication** option box and click on the **Save** button.

Devolutions Passw	Devolutions Password Server Console - Password Server Settings –		
Passwoi	rd Server Settings		
General Database Authentication Domain IIS Advanced	Authentication Modes Authenticate with domain user Authenticate with database user Authenticate with Office365 user Authenticate with local machine user Authenticate with Devolutions Password Server custom user Windows Authentication Image: Enable Windows authentication Image: Windows authentication requires further configuration on your IIS server. Please dick the Help button for instructions.	Ø	
	Search property Save	Can	cel

Server Settings Dialog

2. In the Server Roles, install the Windows Authentication server role.



Add Roles and Features Wizard Dialog

3. Next, open the **IIS Manager**, select the server in the **Tree View** and open the **Feature Delegation** in the **Management** section.

Internet Information Services (IIS)	Manager	
← → VWINDSRV-DVL	LS4 >	
File View Help		
Connections	VWINDSRV-DVLS4 Home	
> 📲 VWINDSRV-DVLS4 (WINDJAN	Filter: • Co • Show All Group by: Area • E •	
	🔏 🧐 🔓 🗊 🏔 🕋 🕋	^
	Authentic Compression Default Directory Error Pages Handler HTTP Document Browsing Mappings Respon	
	📆 🍯 📗 🏂 🐴 🏴 😂	
	ISAPI and ISAPI Filters Logging MIME Types Modules Output Request CGI Restri Caching Filtering	
	Server URL Rewrite Worker Certificates Processes	
	Management	
	Editor Delegation Permissions Users Service Configurat Platfor	*
< >	T Features View 🔄 Content View	
Ready		

IIS Manager

4. Set the Authentication - Anonymous and the Authentication - Windows feature delegation to the value Read/Write.

Internet Information Services (IIS) I	Manager			- 🗆 X
← → ♥ WINDSRV-DVLS	54 🕨			😰 🛛 🏠 🔞 -
File View Help				
Connections	Feature Deleg	gation		Actions Set Feature Delegation
Start Page	Use this feature to configure t	he default delegation state for features at lower levels in IIS Manager.		Read/Write Read Only
Application Pools	Group by: No Grouping	•		Not Delegated
> · o Sites	Name	Delegation	^	Reset to Inherited
	.NET Trust Levels .NET Users	Read/Write Configuration Read/Write		Reset All Delegation Custom Site Delegation
	Application Settings ASP.NET Impersonation	Read/Write Read/Write		Help
	Authentication - Anonymous	s Read/Write		
	Authentication - Basic	Read Only		
	Authentication - Digest	Read Only		
	Authentication - Windows	Read/Write		
	Compression	Read/Write		
	Connection Strings	Read/Write		
	Default Document	Read/Write		
	Directory Browsing	Read/Write		
	Error Pages	Read/Write		
	Feature Delegation	Read/Write	~	
	Eastures View 🕞 Contact	View		
< >		view		
Configuration: 'localhost' applicationH	ost.config			Sec. 19

IIS Manager - Feature Delegation

5. Finally, in the data source configuration of each clients, enable the **Use Windows Authentication** option.

📮 Remote Desktop Man	nager	_		×
Devolu	tions Server			
Connection Settings Pri	ivate Vault Advanced			
Name Server	DVLSAsset_Admin http://VWINDSRV-DVLS4/DVLSAsset		~	٩
	Use Windows authentication			
Username	Always ask username			
Password	Always ask password			
	Test Connection			
ID 1E8290A7-6A72-49	90C-9038-6826D844FB7F O	K	Car	icel

Data Source Configuration Dialog

9.5.10 Enforcing usage of LDAPS

DESCRIPTION

To require that a directory server rejects simple binds which occur on a clear text connection, you must apply a policy.

Please refer to <u>How to enable LDAP signing in Windows Server 2008</u> for the original article, but we will duplicate the content here for ease of use (especially since we hard a hard time finding it ourselves...).

HOW TO CONFIGURE THE DIRECTORY TO REQUIRE LDAP SERVER SIGNING USING GROUP POLICY

HOW TO SET THE SERVER LDAP SIGNING REQUIREMENT

- 1. Click **Start**, click **Run**, type **mmc.exe**, and then click **OK**.
- 2. On the File menu, click Add/Remove Snap-in.
- 3. In the Add or Remove Snap-ins dialog box, click Group Policy Management Editor, and then click Add.
- 4. In the Select Group Policy Object dialog box, click Browse.
- 5. In the **Browse** for a **Group Policy Object** dialog box, click **Default Domain Policy** under the **Domains**, **OUs** and linked **Group Policy Objects** area, and then click **OK**.
- 6. Click Finish.
- 7. Click **OK**.
- 8. Expand Default Domain Controller Policy, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies and then click Security Options.
- 9. Right-click **Domain controller**: **LDAP server signing requirements** and then click **Properties**.
- 10.In the **Domain controller**: LDAP server signing requirements **Properties** dialog box, enable **Define** this policy setting, click to select **Require signing in** the **Define this policy setting** drop-down list, and then click **OK**.
- 11.In the Confirm Setting Change dialog box, click Yes.

HOW TO SET THE CLIENT LDAP SIGNING REQUIREMENT THROUGH LOCAL COMPUTER POLICY

- 1. Click Start, click Run, type mmc.exe, and then click OK.
- 2. On the File menu, click Add/Remove Snap-in.
- 3. In the Add or Remove Snap-ins dialog box, click Group Policy Object Editor, and then click Add.
- 4. Click Finish.

- 5. Click **OK**.
- 6. Expand Local Computer Policy, expand Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
- 7. Right-click **Network security**: **LDAP** client signing requirements, and then click **Properties**.
- 8. In the **Network security**: **LDAP** client signing requirements **Properties** dialog box, click to select **Require signing in** the drop-down list, and then click **OK**.
- 9. In the Confirm Setting Change dialog box, click Yes.

HOW TO SET THE CLIENT LDAP SIGNING REQUIREMENT THROUGH A DOMAIN GROUP POLICY OBJECT

- 1. Click Start, click Run, type mmc.exe, and then click OK.
- 2. On the File menu, click Add/Remove Snap-in.
- 3. In the Add or Remove Snap-ins dialog box, click Group Policy Object Editor, and then click Add.
- 4. Click **Browse**, and then select **Default Domain Policy** (or the **Group Policy Object** for which you want to enable client LDAP signing).
- 5. Click **OK**.
- 6. Click Finish.
- 7. Click Close.
- 8. Click **OK**.
- Expand Default Domain Policy, expand Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Security Options.
- 10.In the **Network security**: **LDAP** client signing requirements **Properties** dialog box, click to select **Require signing in** the drop-down list, and then click **OK**.
- 11.In the Confirm Setting Change dialog box, click Yes.

9.5.11 Identify which Server is answering on a High Availability Topology

DESCRIPTION

The following steps will explain how to define which server is answering when connecting on the Devolutions Password Server web page on a High Availability/Load Balancing topology.

- 1. Open **IIS Manager** on the server where the Devolutions Password Server is hosted.
- 2. Expand the nodes in the **Connections** pane and select the Devolutions Password Server web application.



Connections Pane

3. Open the HTTP Response Headers.



IIS Manager

4. Click on Add... in the Actions pane to add a new HTTP Response Header.

🕞 Internet Information Services (IIS) I	Manager			_		×
← → RIGEL ► Sites	▶ Default Web Site ▶	dvlsorion 🕨			💀 🖂 🏠	• 🕥
<u>F</u> ile <u>V</u> iew <u>H</u> elp						
Connections Start Page Start Page Start Page Sites Si	HTTP Re Use this feature to cor from the Web server. Group by: No Group Name X-Powered-By	esponse Heade nfigure HTTP headers t ping • Value ASP.NET	rs hat are added to responses	Actions Add Set Commo Help	n Headers	
Configuration: 'Default Web Site/dvlso	rion' web.config					• <u>.</u>

HTTP Response Headers

5. Enter a **Name** and a **Value** that will identify the server. Then click on **OK** to save this information.

Add Custom HTTP Response Header	?	×
Name:		
X-Server-Name		
Value:		
Rigel-Server1		
ОК	Cancel	

Edit Custom HTTP Response Headers Dialog

- 6. Repeat steps 1 to 5 on each server of your **High Availability/Load Balancing** cluster. It is important to set a different value for each server but keeping the same **Name**.
- 7. Open your favorite browser.

- 8. Open the **Developer Tools** in the browser. Usually the **F12** key will open the **Developer Tools** in **Google Chrome**, **Firefox** or **Microsoft Edge**.
- 9. Browse to your Devolutions Password Server web page.
- 10.Using **Firefox**, in the **Network** tab, you should found the **Custom HTTP Response Header** value of the answering server of the cluster.

				D Lo	Devoluti Password	ons d Server account	
				Username		*	
				Password		*	
	Dinspector	Console 🕞 Debug	jger {}S	tyle Editor 🖉 Pe	erformance 🕕 Memor	y 🔄 Network 😫 Storage	🚇 Adblock Plus 🛛 🕁 🚥 🗙
Ŵ	∀ Filter URLs		1	All HTML C	CSS JS XHR Fonts I	mages Media WS Other [Persist Logs 🗹 Disable cache 🛛 No throttling 🗘 HAR 🗘
Stat	us Method	F Cause	Туре	Transferred	Size 0 ms	1.28 s 2.56 s 3.84	Headers Cookies Params Response
200	GET	login document	html	3.04 KB	2.76 KB	→ 1700 ms	Request URL: http://rigel.orion.loc/dvlsorion
200	GET	styles.d stylesheet	CSS	221.93 KB	221.60 KB	➡ 159 ms	Remote address: 192.168.4.18:80
200	GET	runtim script	js	2.45 KB	2.12 KB	i → 69 ms	Status code: 200 ⑦ Edit and Resend Raw headers
200	GET	polyfillsscript	js	145.71 KB	145.37 KB	→ 145 ms	Version: HTTP/1.1
200	GET	scripts script	js	304.97 KB	304.63 KB	→ 202 ms	♥ Filter headers
200	GET	main.6 script	js	3.40 MB	3.40 MB	→ 553 ms	Content-Type: text/html; charset=utf-8
200	GET	css?fa stylesheet	CSS	1.13 KB	9.30 KB	I → 30 ms	(7) Date: Tue, 17 Jul 2018 15:25:48 GMT (2) Expires: -1
200	GET	mem8Yfont	woff2	14.11 KB	13.72 KB	I → 7 ms	Pragma: no-cache
200	GET	devolutfont	octet-stre	. 140.92 KB	140.58 KB	→ 17 ms	③ Server: Microsoft-IIS/10.0
200	GET	login-b img	jpeg	189.97 KB	189.64 KB	→ 20 ms	X-AspNet-Version: 4.0.30319
200	GET	en_US.j xhr	json	743.53 KB	743.20 KB	→ 70 ms	X-Powered-By: ASP.NET
200	GET	mem5Yfont	woff2	14.77 KB	14.38 KB	→ 10 ms	X-Server-Name: Rigel-Server1
200	GET	is-loggedxhr	json	323 B	5 B	- 2(🗸	Kequest headers (383 B)
Ø	17 requests 5.16	MB / 5.15 MB transferre	d Finish:	4.08 s DOMCont	entLoaded: 3.22 s load:	4.10 s	plication/xntrii,application/xntrii+xm

Firefox Developer Tools - Network Tab

9.5.12 Manage Encryption Keys on a High Availability Topology

DESCRIPTION

The encryption keys must be the same of each Devolutions Password Server instances of your High Availability Topology.

We recommend to do a backup of the SQL database before any operation that could modify the information of the SQL database. During this operation, all users must be in offline mode or disconnected from the Devolutions Password Server data source to avoid data loss.

Here are the steps to manage the encryption keys on that specific environment. If you have to upgrade Devolutions Password Server, please upgrade one instance at a time.

- 1. Open the Devolutions Password Server Console on the first server.
- 2. Open the menu on the right of the Devolutions Password Server Console and click on **Manage Encryption Keys**.

😂 i 🛊 🏚 🗟 🕅	j 😼 📑 🔇	🧰 I 🛃							
Actions	Name	Web Application Name	Version	Expiration	Website	Runtime Version	Path	٥	Diagnostic
///	DVLS Local	/dvls	4.6.1.0	No expiration	Default Web Site		C:\inetpub\wwwroot\d\	1	Send Diagnostic to Support
									View Installation Logs
Edit									Open Backup Folder
								9	Manage Encryption Keys
								ŝ	Register As a Local Data Source
New									View Web API Help

Devolutions Password Server Console

📮 Remote D	esktop N	/lanager	×
E N	lana	ge Encryption Keys	
Operati	ion	Export ~	
		🗹 Login Key	
		🗹 Token Storage Key	
		Attachment Storage Key	
		Password Storage Key	
		Security provider configuration	
Passwo	ord	•••••	
		OK Cance	I

3. Set the **Operation** to **Export**, enter a password and click on the **OK** button.

Manage Encryption Keys Dialog

Remote Desktop N	Manager					×
← → • ↑ <mark> </mark>	$\rightarrow~$ This PC $\rightarrow~$ OS (C:) $\rightarrow~$	Temp >	~	ට Search Temp		<i>م</i>
Organize 🔻 Ne	w folder					?
🎉 Support Requ	iest ^ Name	^	Date modified	Туре	Size	
\land OneDrive	temp		2017-03-29 3:25 PM	File folder		
💻 This PC						
📃 Desktop						
🔮 Documents						
👆 Downloads						
🎝 Music						
Pictures						
📑 Videos						
🟪 OS (C:)						
👝 TempDrive (D);)					
💣 Network	v					
File name:	EncryptionKeys.bin					~
Save as type:	(*.bin)					~
∧ Hide Folders				Save	Cancel	

4. Select a folder where to save the file and click on the **Save** button.

- 5. **Copy** the encryption file on the other server.
- 6. If you need to upgrade the second server, you must do it before going any further with the following steps.
- 7. Go on another server where Devolutions Password Server is hosted and open the **File Explorer** in the **App_Data subfolder** of your web application folder. **Delete** every encryption file you will find in that subfolder.



8. Open the Devolutions Password Server Console on the server. Then, open the Advanced menu on the right of the Devolutions Password Server Console and click on Manage Encryption Keys.

C 🕴 🏚 📑 🕷	s i 😼 💽 🔇) 🛱 🛃								
Actions	Name	Web Application Name	Version	Expiration	Website	Runtime Version	Path	Ð	Diagnostic	
///	DVLS Local	/dvls	4.6.1.0	No expiration	Default Web Site		C:\inetpub\wwwroot\d	vl	Send Diagnostic to Support	
<i>S</i>									View Installation Logs	
Edit									Open Backup Folder	
								Ç,	Manage Encryption Keys	
-								ß	Register As a Local Data Sou	irce
New									View Web API Help	
			Devolu	utions Pa	assword S	erver Cor	nsole			

9. Set the **Operation** to **Import** and click on the **OK** button.

📮 Remote Desktop	o Manager 💦 🖓	×
🚺 Man	age Encryption Keys	
Operation	Import ~	
	🗹 Login Key	
	✓ Token Storage Key	
	Attachment Storage Key	
	Password Storage Key	
	Security provider configuration	
	OK Cancel	

Manage Encryption Keys Dialog

10.Select the encryption file and click on the **Open** button.

📮 Remote Desktop Mar	nager							×
	This PC	> OS (C:) > Temp >	~	Ō	Search Temp			<i>م</i>
Organize 🔻 New f	folder							?
💻 This PC	^ N	ame	Date modified	Туре		Size		
E. Desktop		n temp	2017-03-29 3:25 PM	File fo	older			
Documents		EncryptionKeys.bin	2017-08-10 4:18 PM	BIN F	ile		2 KB	
👆 Downloads								
b Music								
Pictures								
🚆 Videos								
🟪 OS (C:)								
🕳 TempDrive (D:)	~							
Fi	ile name:	EncryptionKeys.bin		~	(*.bin)			\sim
					Open		Cancel	

Select the encryption file

11.Enter the password and click on the **OK** button.

📮 Remote Desktop Manager	×
Import Encryption Keys	
Password •••••	
OK Cance	ł

12.Click on the **Yes** button on the **Change encryption keys** warning dialog. Because the encryption keys was deleted, this operation will not be completed on the database. It will use the same encryption keys as the other server.

Import Encryption Keys password Dialog



Change Encryption Keys Warning Dialog

9.5.13 Ports And Firewalls

DESCRIPTION

Devolutions Password Server in itself does not dictate which ports to use for any of the resources that it accesses. You must consult with your system administrator to ascertain which adjustments need to be made in order for the system to inter-operate with your infrastructure.

INBOUND

The only inbound port that is needed for Devolutions Password Server is for http or https communication, as per your preference. We strongly recommend using https even if only within your own network infrastructure. Although the default port is easily changed, it is typically port 443.

OUTBOUND

Two technologies are in play for proper operation of Devolutions Password Server : SQL Server, LDAP.

SQL SERVER

Depending on the choice of **Default Instance** or **Named Instance** that was made during the installation, the SQL Server instance will listen on different ports.

Using SQL Server Configuration Manager, you can see the details in the Protocols section



Sql Server Configuration Manager - Protocol details

In most cases, TCP/IP will be used for remote connections. You will be able to see what ports are in use. If you see that TCP Dynamic Ports are in play, they will change upon every restart of the SQL Server instance and therefore are **not a good fit** for a hardened installation.

TCP/IP Properties	?	×
Protocol IP Addresses		
Active Yes		
Enabled No		
IP Address 192.168.1.100		
TCP Dynamic Ports		
TCP Port 1433 -		•
IP4		
IPAII		
TCP Dynamic Ports		
TCP Port 1433 <		•
IP2		
OK Cancel Apply	H	Help

TCP/IP Properties

For more information please consult SQL Server Configuration Manager on Technet

LDAP/LDAPS

As indicated in <u>LDAPS on Technet</u>, LDAP communications are by nature insecure under certain conditions:

By default, LDAP communications between client and server applications are not encrypted. This means that it would be possible to use a network monitoring device or software and view the communications traveling between LDAP client and server computers. This is especially problematic when an LDAP simple bind is used because credentials (username and password) is passed over the network unencrypted. This could quickly lead to the compromise of credentials.

Follow the instructions for your operating system in order to establish LDAPS. It will involve deploying certificates generated using your of **Certification Authority (CA)**.

LDAP by default uses port 389. Even when you enable LDAPS, it may use plain LDAP therefore it needs to be disabled, please consult <u>Enforcing usage of LDAPS</u>.

LDAPS by default uses port 636 for typical domains, but will use port 3269 when communicating with a **Global Catalog Server** (basically when you have a Forest). Your domain administrator should be able to provide you with details of your domain infrastructure, especially if custom ports were used. You can also use ldp.exe to perform connectivity tests.

9.5.14 Switch from Shared passphrase to Shared passphrase (v2)

DESCRIPTION



We should deprecate the Shared passphrase v1 Security Provider so we highly recommend to remove the Shared passphrase v1 and set the Shared passphrase (v2).



The method to know which version of the Shared passphrase is set as the **Security Provider**, if there is no version displayed, it is version 1.

Here are the steps to modify the **Security Provider** set on the Devolutions Password Server instance from **Shared passphrase** to **Shared passphrase (v2)**.

- 1. Ensure that the instance users have the offline mode enabled and that they all perform a **Full Refresh** of the cache (CTRL+F5).
- 2. Have your team switch to the offline mode, allowing them to work while the system is down.
- 3. Perform a full backup of the database.
- 4. Open the Devolutions Password Server Console and switch the instance to offline mode with the **Go Offline** button.

E	D)evoluti	ons S	erv	er Console				_	×
ວ		ê 🍺		1	鸟 Import Users 🔋	🎓 🛃 😰 🕙 🔁 😵 🔚				:
A	ctic	ons			Details					
					Name	Devolutions Server	Version	5.0.1.0		
					Description					
		Cult			Server serial	XXXXX-XXXXX-XXXXX-XXXXX-29H54	Corporate Edition			
		4.					No expiration - subso	cription license		
		Now								
		INEW								
		$\mathbf{\mathbf{v}}$			Website	Default Web Site	Web application	/dvls		
				÷	Default path	C:\inetpub\wwwroot\dvls				
	De	elete			Application pool	dvls	Runtime	v4.0		
F		_			Authentication	Domain, DVLS Custom				
		- 🌮			Scheduler service	Stopped				
ų	pgra	ade Serv	/er				Go Offline	+		
		¢.,								
	U Sc	ninstall heduler								
5	i.o.:	2.0								

Devolutions Password Server Console

5. Open the **Security Providers** dialog from the toolbar.

Devolutions Set	erver Console			
🕽 🕴 🏚 🗃	😵 🦂 Import Users	n 🔁 🖉 🔁 🖓 📑 📚 🗄	ਤ ਤ	
Actions	Details	Manago cogurity provider		
_//	Name	Devolutions Server	Version	5.0.1.0

Devolutions Password Server Console toolbar

6. Select the **Default** item to remove the **Security Provider Passphrase v1** and click on **Apply**.

Devolutions Server Console - Security Provider — 🗆 🗙								
Security Provider								
Security type Default Apply Cancel This is default security mode. The Xml is not encrypted by default. The session must be configured to enable the encryption. Please note that the password are always encrypted.								
		Clo	se					
Security Provider Dialog								

Devolutio	ons Server Console X
	All data source sessions will be processed with the new security provider. Prior to running this process, please verify that no one is editing or adding any session.
?	WARNING! Historical version history detail information will not be available for comparison once you've applied the new security provider settings.
	Are you ready to apply the new security provider settings?
	Yes No

Security Provider confirmation Dialog

7. Switch the instance in online mode and check some entries with Remote Desktop Manager to ensure that the information is still accessible.

Devolutions Se	erver Console				_	×
こ 🕯 👼 🔒 🤅	🐉 💪 Import Users 🏾 🕞	🎓 😎 😰 🖺 😫 🐑				:
Actions	Details					
	Name	Devolutions Server	Version	5.0.1.0		
Edit	Description					
	Server serial	XXXXX-XXXXX-XXXXX-XXXXX-29H54	Corporate Edition			
+			No expiration - subso	cription license		
New						
	Website	Default Web Site	Web application	/dvls		
	: Default path	C:\inetpub\wwwroot\dvls				
Delete	Application pool	dvls	Runtime	v4.0		
	Authentication	Domain, DVLS Custom				
	Scheduler service	Running				
Upgrade Server	1s offline		Go Online	+		
0						
Uninstall Scheduler						
5.0.2.0						

Devolutions Password Server Console

- 8. Switch back to offline mode.
- 9. Perform another backup so if the next steps fail the previous operation will not be lost.
- 10.Open the **Security Provider** dialog and set the **Shared passphrase (v2)** to encrypt your data.

Devolutions Server Console - Security Provider	—		×
Security Provider			
Security type Shared passphrase (v2) Apply Cancel This security provider encrypt the whole Xml us passphrase mixed to a private key. The passphrase non each machine.	ing AES w irase will b	ith a e asked o	nce
		Clo	se

Security Provider Dialog

- 11.Switch back to online mode.
- 12.Check some entries with Remote Desktop Manager to ensure that the information is still accessible.
- 13.On success, the backups taken during the process can be deleted.

9.5.15 SQL Server Express configuration

DESCRIPTION

To be able to connect to a SQL database with Devolutions Password Server, here is the suggested configuration in Microsoft SQL Server Express Edition.

STEPS

Most of our customers use the mixed mode Server Authentication. As per Microsoft, it is not the safest authentication method to use with Microsoft SQL Server Express Edition but we recommend to use it to configure and test your Devolutions Password Server instance. After a successful installation of Devolutions Password Server, you can set it back to Windows Authentication mode and set the Integrated Security option in the Database tab of the Devolutions Password Server Server Settings. Consult this topic on How to Configure Devolutions Password Server to use integrated security. To enable the mixed mode, in the Microsoft SQL Server **Management Studio**, open the properties dialog of your server and go in the **Security** tab. Then, select the SQL Server and **Windows Authentication** mode option.

📑 Microsoft SQL Server M	lanagement Studio	
File Edit View Debug	Tools Window Help	
G - O 📅 - 눱 - 🗳	🕽 🔛 📲 🛄 New Query 📑	B B K 山 台 タ・ペ・ 編
Object Explorer Connect - PP P DEVOLUTIONS70 SQL Databases Security Security Server Objects Replication Management	C S EXPRESS2016 (SQL Server 13.0.172 Server Properties - DEVOLUT Select a page General Memory Processors Secury Tonnections Database Settings Advanced Permissions	
		None Failed logins only Successful logins only Both failed and successful logins Server proxy account
	Connection	Enable server proxy account
	Server: DEVOLUTIONS70\SQLEXPRESS Connection: DEVOLUTIONS70\epointer	Proxy account: Password:
	Wew connection properties	Enable C2 audit tracing Cross database ownership chaining
	Progress Ready	
		OK Cancel

The next option that needs to be activated is the **Allow remote connections to this server** option. You will find that option in the **Connections** tab of the SQL Server **Properties** dialog. Then, click on the **OK** button to save the modifications.

Server Properties - DEVOLU	_		\times	
Select a page Page General	🖾 Script 🔻 🚺 Help			
Memory Processors Connections Database Settings Advanced Permissions	Connections Maximum number of concurrent connections (0 = unlimited): Use query governor to prevent long-running queries Default connection options:			
Connection	implicit transactions cursor close on commit ansi warnings ansi padding ANSI NULLS ANSI NULLS			
Connection	anthmetic abort			~
DEVOLUTIONS70\SQLEXPRESS	Remote server connections			
Connection:	Allow remote connections to this server			
DEVOLUTIONS /0\epointer	Remote auerv timeout (in seconds, 0 = no timeout):			
View connection properties	600			
	Require distributed transactions for server-to-server communication			
Progress				
Ready	Configured values O Running values			
		ОК	Car	ncel

Finally, the **SQL Server Browser** service must be started on the machine where the SQL Server is hosted. Please run services.**msc** and look for the **SQL Server Browser** in the list.

🔍 Services				_	
File Action View	Help				
	à 📑 🛛 🖬 🕨 🔲 II 🕨				
Services (Local)	Name	Description	Status	Startup Type	Log On / ^
	🤹 Spot Verifier	Verifies potential file system corruptions.		Manual (Trig	Local Sys
	🖏 SQL Full-text Filter Daemon Laun	Service to launch full-text filter daemon pr	Running	Manual	NT Servie
	🤹 SQL Server (SQLEXPRESS2016)	Provides storage, processing and controlle	Running	Automatic	NT Servie
	SQL Server Agent (SQLEXPRESS2	Executes jobs, monitors SQL Server, fires al		Disabled	Network
	🖏 SQL Server Browser	Provides SQL Server connection informati	Running	Automatic	Local Ser
	3QL Server CEIP service (SQLEXP	CEIP service for 3qi server	Running	Automatic	INT Servi
	🤹 SQL Server Launchpad (SQLEXPR	Service to launch Advanced Analytics Exte	Running	Automatic	NT Servi
	SQL Server Reporting Services (S	Manages, executes, renders, schedules an	Running	Automatic	NT Servie
	🖏 SQL Server VSS Writer	Provides the interface to backup/restore	Running	Automatic	Local Sys
	SSDP Discovery	Discovers networked devices and services	Running	Manual	Local Ser
	🖏 State Repository Service	Provides required infrastructure support f	Running	Manual	Local Sys
	Still Image Acquisition Events	Launches applications associated with still		Manual	Local Sys
	🖏 Storage Service	Provides enabling services for storage setti	Running	Manual (Trig	Local Sys
	K T 14				- 16 T
	Extended Standard				

We recommend to set the **Startup** type to **Automatic** for the **SQL Server Browser** service. Double-click on the service to open the **Properties** dialog. Then start the service by clicking on the **Start** button and select **Automatic** in the **Startup** type drop down menu. Finally, click on the **OK** button.

SQL Serve	er Browse	er Properties	s (Local C	Compu	ter)		×
General	Log On	Recovery	Depende	encies			
Service	name:	SQLBrowse	er				
Display	name:	SQL Serve	r Browser				
Description: Provides SQL Server connection information to client computers.							$\hat{}$
Path to "C:\Pro	executabl gram Files	e: (x86)\Micros	soft SQL (Server\	0\Shared	\sqlbrowser.	exe"
Startup	type:	Automatic					~
Service	status:	Running					_
9	Start	Stop		Pau	use	Resume	е
You car from he	n specify t re.	he start para	meters tha	at apply	when you	start the sen	/ice
Start pa	arameters:						
			ОК		Cance	/	Apply

9.5.16 Update your registration serial after a renewal

DESCRIPTION

Devolutions Password Server is licensed as a yearly subscription which must be kept up-to-date. A new license key is provided when you renew. The new license key needs to be entered in the Devolutions Password Server Console.



Your data is always available even if the subscription has expired. You simply need to connect directly to that database using a SQL Server data source.

SETTINGS
Open the renewal email. The email includes your licenses. In the example, (a) the user CAL license serial specifies the number of users who can access Devolutions Password Server. The second serial (b) is for your Devolutions Password Server.

Greetings customer, Below, you will find your unique license(s) information.	
a Devolutions Password Server User: (15 users) Serial: -EPG57 Renewal Date: February 1st 2020	
Download 🕁	
Register your License and Get Started »	
Devolutions Password Server User: Serial: Renewal Date: February 1st 2020	
Download 🕁	
Register your License and Get Started »	

License Renewal Information

- 2. Open the Devolutions Password Server Console on the machine where you installed Devolutions Password Server.
- 3. To access Password Server Settings, click Edit.

Devolutions Pass	sword Server Console			_		×
C 🕴 🏚 🗟 🍪	- 🕞 🍘 😰 😰 🖓 🗮 📚	⊠ ⊠				:
Actions	Details					
	Name	Devolutions Password Server	Version	6.0.1.	0	
Edit	Description					
	Serial (server)	XXXXX-XXXXXX-XXXXX-XXXXX-3DW71	None			
			Friday, November 1, 2019			
New	Serial (user CAL)	XXXXX-XXXXX-XXXXX-XXXXX-LPI50	6125			
X	Website	Default Web Site	Web application	/DVLS		
Delete	Default path	C: \inetpub \wwwroot \DVLS				
	Application pool	DVLS	Runtime version	v4.0		
	Authentication	DVLS Custom, Database				
Upgrade Server	Scheduler service	Running		_		
			Go Offline			
Ф _о						
Uninstall Scheduler						
6.1.0.0						

Devolutions Password Server Console

- 4. Enter the Server serial you received in the renewal email in the Server field.
- 5. Enter the **User CAL Serial**. This serial specifies the number of users who can access Devolutions Password Server.
- 6. Enter the **Launcher CAL** if you are opening remote connections through the web interface with Devolutions Launcher.

Devolutions Password	Devolutions Password Server Console - Password Server Settings -							
Passwo	rd Server Sett	tings						
General	General							
Database								
Authentication	Name	Devolutions Password Server						
Two-Factor	Description	Windjammer Local						
Security								
GeoIP Security		Enable new version mode						
IIS	Serial							
Email								
Logging	Server 4	Re	equest Tr	<u>ial</u>				
Features	User CAL 5	61	125					
Scheduler	Laurenter Cal							
Advanced	Launcher CAL							
	Information							
	Edition	None						
	Expiration	Friday, November 1, 2019						
	Search property	<u>A</u>		Save	Can	cel		

Server Settings -- General

9.5.17 User Agent

USER AGENT OF REMOTE DESKTOP MANAGER ENTERPRISE EDITION FOR WINDOWS

The **User Agent** used by Remote Desktop Manager Enterprise Edition for Windows when it connects to Devolutions Password Server is:

Mozilla/4.0+(compatible;+MSIE+6.0; +MS+Web+Services+Client+Protocol+4.0.30319.42000)

9.6 Troubleshooting

9.6.1 After Upgrading Server the Devolutions Password Server is Empty

DESCRIPTION

You have attempted to upgrade your **Devolutions Password Server instance** and the upgrade was not completed correctly. Now, your instance is not present in the **Devolutions Password Server Console** and your data source is not connected.

🟓 ╢ 🥒 🕽 🔍 Quick <	Host>	v 🐼 💉	🔒 🔻 Dev	olutions Server - Console - F	lemote Des	ctop Manager			0	<u>n</u> –		×
FILE HOME ACTIONS	EDIT VIEW	ADMINISTRATION	REFACTORIN	IG TOOLS WINDOW	/ HELP						7 -	^
Online Register Help Version Help	View Application	on Log Diagnostic Pro	filer Record	Contact Us Visit our Forum View the Change History	Blog	 Facebook Twitter Spiceworks Follow Us 	in LinkedIn Houtube Google+	 Check Version Upgrade to Enterprise Edition About 	() About			
Navigation	ųх	😢 Dashboard	Devolutions	Server - Console X								
	<i>A</i>	I/XC 🖢	🛔 Users 🝺	Security Groups 报 Role	s 🔇	8 📄 🖣 🖸	1					
	¥	Name		Web Application Name	Version	Expiration	Websi	te Runtime Version	n Path			
Name												
Not connected												
		<			_							>
<search></search>	▼ ··· × 0E	INTRY										

Devolutions Server Console empty

INSTRUCTIONS

- 1. Navigate to the %*temp*%*RDM* folder and <u>copy the content of the folder</u>.
- 2. Navigate to the folder where your Devolutions Password Server was deployed originally and **paste** the content of *%temp%\RDM* inside.
- 3. If you close and reopen your Devolutions Password Server Console, your instance should be present.
- 4. You can now proceed again with the upgrade of your server.

If the files are not present or the solution doesn't work, you will need to restore the backup that you have created in the preparation phase as described in <u>Upgrading</u> <u>Devolutions Password Server</u>

9.6.2 Blank login page on a Windows Server 2016

DESCRIPTION

When you open the web page of the Devolutions Password Server instance that is hosted on a Windows Server 2016, **the web page is blank**.

STEPS

- 1. Open the **IIS Manager** on the server.
- 2. Expand the root and select **Application Pools**.



3. Select the Devolutions Password Server application pool and click on **Advanced Settings**... in the Actions pane on the right.

💐 Internet Information Services (IIS) Manager								-		×
← → ② ► VWINDSRV-DVLS4 ► Applica	tion Pools								🌆 🔤 🙆	• 🔞 •
File View Help										
File View Help Connections Start Page Start Page Start Page Start Start Start Page Start Start S	Applicat This page lets you view associated with worke applications. Filter: Name MET v2.0 MET v2.0 MET v2.0 Classic MET v4.5 Classic Classic .NET v4.5 Classic Classic .NET v4.5 DefaultAppPool DVLSAuge DVLSAuge DVLSAuge DVLSWebCreati	ion Poo y and man processes Status Started Started Started Started Started Started Started Started Started Started Started Started Started	DIS age the list of ag , contain one or .NET CLR V v2.0 v4.0 v4.0 v4.0 v4.0 v4.0 v4.0 v4.0 v4	plication pools on more applications, w All Group by: Managed Pipel Integrated Classic Integrated Integrated Integrated Integrated Integrated Integrated Integrated	the server. Application and provide isolation No Grouping Identity ApplicationPoolld ApplicationPoolld ApplicationPoolld ApplicationPoolld ApplicationPoolld NetworkService NetworkService NetworkService	pools are among different Applications 0 0 0 0 1 1 1 1 1	Ac	tions Add Applica Set Applica Start Stop Recycle Edit Applic Basic Settin Recycling Advanced 5 Rename Remove View Applic Help	ation Pool tion Pool D Pool Tasks ation Pool gs ettings ations	efaults
Ready	Features View	ontent Vie	w							€≣.:

IIS - Application Pools

4. Set the Enable 32-Bit Applications to the value True.

~	(General)	^					
Ť	NET CLR Version	v4.0					
Г	Enable 32-Bit Applications	True					
Ŀ	Managed Pipeline Mode	Integrated					
	Name	DVLS2016					
	Queue Length	1000					
	Start Mode	OnDemand					
~	CPU						
	Limit (percent)	0					
	Limit Action	NoAction					
	Limit Interval (minutes)	5					
	NUMA Node Affinity Mode	Soft					
	NUMA Node Assignment	MostAvailableMemory					
	Processor Affinity Enabled	False					
	Processor Affinity Mask	4294967295					
	Processor Affinity Mask (64-bit c	4294967295					
	Processor Group	0					
~	Process Model						
>	Generate Process Model Event L	>					
En	able 32-Bit Applications						
[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mo							

Advanced Settings Dialog

9.6.3 Duplicate Devolutions Password Server instance

DESCRIPTION

When you open the Devolutions Password Server Console, two instances of the same Devolutions Password Server are visible in the console. One with only a "/" as the Web Application Name.

🔁 Dashboard	Devolutions Serve	er-Console ×						
🖸 🚦 Users 🕅 Security Groups 设 Roles 📰 🛞 🛅 👼 🖬 😨								
Actions	Name	Web Application Name	Version	Expiration	Website	Runtime Version	Path	
	Devolutions Server	/ /DVLS	4.0.11.0 4.0.11.0	2017-03-18	Default Web Site Default Web Site	v4.0	C: \inetpub \wwwroot \DVLS C: \inetpub \wwwroot \DVLS	
Devolutions Password Server Console								

CAUSE 1

Using the default parameters of the IIS Manager, the Default Web Site points to the same Physical Path of the Devolutions Password Server web application.

STEPS

Change the the path of the Web Site in the IIS Manager.

1. Open **IIS Manager**, select the **Web Site** that contains the Devolutions Password Server web application and click on **Advanced Settings** in the Actions panel on the right.



IIS Manager

2. Change the **Physical Path** of the Web Site from the Devolutions Password Server subfolder to the parent folder.

Adva	nced Settings		?	×
~	(General)			
	Application Pool	Default Web Site		
	Bindings	http:*:80:		
	ID	1		
	Name	Default Web Site		
	Physical Path	C:\inetpub\wwwroot\DVLS		
15	Physical Path Credentials			
	Physical Path Credentials Logon Type	ClearText		
	Preload Enabled	False		
~	Behavior			
	Enabled Protocols	http		
>	Limits			
Ph [pł	ysical Path nysicalPath] Physical path to the content for the v	irtual directory.		
		ОК	Cance	l

Web Site Advanced Settings - Before the Physical Path modification

~	(General)		
	Application Pool	Default Web Site	
	Bindings	http:*:80:	
	ID	1	
	Name	• Default Web Site	
	Physical Path	C:\inetpub\wwwroot	[
	Physical Path Credentials		
	Physical Path Credentials Logon Type	ClearText	
	Preload Enabled	False	
,	Behavior		
	Enabled Protocols	http	
	Limits		
'n	ysical Path		

3. Restart your IIS Server.

💐 Internet Information Services (IIS) Manager		– 🗆 X
← → DEVOLUTIONS70 →		🖸 🛛 🟠 🔞 🕶
File View Help		
Connections	DEVOLUTIONS70 Home	Actions Manage Server
DEVOLUTIONS70 (DEVOLUTIONS70\epoirier) Application Pools Sites	Filter: 	<u>Restart</u> Start Ston
✓	NET NET NET Error NET NET Trut	View Application Pools View Sites
> - Client1.0.0-39	Authorizat Compilation Pages Globalization Levels	Change .NET Framework Version
> · C DBScripts > · DVLS	Application Connection Machine Key Pages and Providers	Get New Web Platform Components
	IIS Manager	

4. On the Devolutions Password Server Console, click on the **Refresh** button and just one instance should be displayed.



Devolutions Password Server Console

CAUSE 2

When the Web Site is located in a different folder then the default one used by the IIS Manager, the Web Site points to the same Physical Path of the Devolutions Password Server web application.

😤 Dashboard	Devolutions Serve	er-Console ×						
😂 🔓 Users 👼 Security Groups 🔮 Roles 📰 🚫 🚎 👼 🗃 📚								
Actions	Name	Web Application Name	Version	Expiration	Website	Runtime Version	Path	
	Devolutions Server	1	4.0.13.0	2017-03-18	Default Web Site		C:\WebSite	
	Devolutions Server	/DVLS	4.0.13.0	2017-03-18	Default Web Site	v4.0	C:\WebSite	

Devolutions Password Server Console

STEPS

To have only one Devolutions Password Server instance without any duplicate, the Physical path of the instance must be points to a subfolder of the Web Site Physical Path.

1. **Open the Windows Explorer** and create a folder in the **Physical Path** of the Web Site. In the image below, the name of the new folder is DVLS. It can be another folder name that fits your needs.



2. Move the selected files and folders into that new subfolder, i.e. DVLS.

📙 🛃 🚽 WebSite			
File Home Share View			
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This PC \rightarrow OS (C:) \rightarrow	WebSite		
ProgramData	Name ^	Date modified	Type Size
Recovery	🗹 📙 App_Data	2017-03-06 1:17 PM	File folder
SQLServer2016Media	🗹 📙 bin	2017-03-06 1:16 PM	File folder
	🗹 📙 client1.0.0-40	2017-03-06 1:17 PM	File folder
Tools	🗹 📙 Custom	2017-03-06 1:16 PM	File folder
Users	DBScripts	2017-03-06 1:16 PM	File folder
WebSite	DVLS	2017-03-06 1:33 PM	File folder
	🗹 📙 Images	2017-03-06 1:16 PM	File folder
	🗹 📙 Scripts	2017-03-06 1:17 PM	File folder
bin	🗹 📙 Templates	2017-03-06 1:17 PM	File folder
client1.0.0-40	🗹 🖪 favicon.ico	2016-08-30 11:00	lcon
Custom	🗹 🖻 favicon.png	2016-09-18 10:52	PNG File
DBScripts	🗹 👷 Global.asax	2015-01-18 3:34 PM	ASP.NET Server A
DVLS	🗹 🖶 ImageBytes.ashx	2016-10-17 7:36 PM	ASP.NET Generic
Images	🖂 🌐 index.aspx	2017-03-03 9:31 AM	ASP.NET Server Pa
Coninta	robot.txt	2013-03-15 3:51 PM	Text Document
Scripts	ServerInfo.ashx	2015-11-11 11:24	ASP.NET Generic
	V 🖓 web.config	2017-03-06 1:17 PM	XML Configuratio
Windows			

Windows Explorer

3. Open the IIS Manager and select the Devolutions Password Server web application in the **Tree View** and click on **Advanced Settings** in the Action panel on the right.



IIS Manager

4. Change the Physical Path to point to the new folder created in step 1.

Adv	anced Settings			?	×		
~	(General)						
	Application Pool	DVLS					
Г	Physical Path	C:\WebSite\DVLS					
15	Physical Path Credentials						
	Physical Path Credentials Logon Type	ClearText					
	Preload Enabled	False					
	Virtual Path	/DVLS					
~	Behavior						
	Enabled Protocols	http					
PL	urical Dath						
Ph [m]	ysical Path Deviced eath to the content for	the virtual directory					
[p							
			ОК	Cance	I		
	Advanced Settings Dialog						

5. To restart your IIS Server, select the root in the **Tree View** and click on **Restart** in the Actions panel on the right.



6. On the Devolutions Password Server Console, click on the **Refresh** button and just one instance should be displayed.

😵 Dashboard	Devolutions Serve	er - Console X					
😂 🛔 Users 👼 S	😂 🔓 Users 👼 Security Groups 设 Roles 📰 🛞 🥽 📑 😨 😪						
Actions	Name	Web Application Name	Version	Expiration	Website	Runtime Version	Path
	Devolutions Server	/DVLS	4.0.13.0	2017-03-18	Default Web Site	v4.0	C:\WebSite\DVLS

Devolutions Password Server Console

9.6.4 Error Uploading Document

DESCRIPTION

You get a HTTP 413 error when trying to upload or attach a document to an existing entry.

Error message dialog			
e request failed with HTTP status 413: Request l	Entity Too Large.		
erprise Edition 11.7.6.0	Memory usage: 479 MB		
ining since: 3 min 18 sec	WebException		
ige			
Stepulon - The request railed with PTTP status 415 ystem. Web.Services. Protocols.SoapHttpClientProt ivevolutions. RemoteDesktopManager. RbuSiness. Data Devolutions. RemoteDesktopManager. Business. Data Devolutions. RemoteDesktopManager. Business. Data Devolutions. RemoteDesktopManager. Business. Data Devolutions. RemoteDesktopManager. Business. Data Devolutions. RemoteDesktopManager. Frames. Freakt Devolutions. RemoteDesktopManager. Frames. Freakt System. Windows. Forms. ToolStripItem. HandleClick(yistem. Windows. Forms. ToolStripItem. FireEventInte yistem. Windows. Forms. ToolStripItem. FireEventInte yistem. Windows. Forms. CoolStripItem. FireEventItes yistem. Windows. Forms. CoolStripItem. FireEventItes yistem. Windows. Forms. CoolStrip. WndProc(Message Devolutions. RemoteDesktopManager. Control. S. Enha yistem. Windows. Forms. CoolStrip. WndProc(Message Devolutions. RemoteDesktopManager. Control. S. Enha yistem. Windows. Forms. Control. Control. NativeWinc System. Windows. Forms. NativeWindow. Callback(Int	s: nequest entity 100 carge. ocol.ReadResponse(SoapClientMessage message, WebResponse response, Stream r ocol.Invoke(String methodName, Object[] parameters) IDMSServices.SaveAttachmentDocument(String connectionID, String attachmentD), Sources.RDMSWebServiceClient.cs47202cb525aa20096c1b71500409b4.c30b7b8838 sources.RDMSWebServiceClient.c5476c72053Cod60a62abeeaa43ff[cb75a0a5d15 sources.RDMSWebServiceClient.SaveAttachmentDocument(String connectionID, SaSources.RDMSWebServiceClient.SaveAttachmentDocument(String connectionID, SaSources.RDMSWebServiceClient.SaveAttachmentDocument(String connectionID, SaSources.RDMSAttachmentSubDataSource.SaveAttachment(AttachmentItem attach tachmentList.ca86a486544123727a1e5c97349462074() tachmentList.ca86a486544123727a1e5c97349462074() tachmentList.ca86a486544123727a1e5c97349462074() tachmentList.ca86a486544123727a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a48654412377a1e5c97349462074() tachmentList.ca86a486544123451861c13e4238215df04b972(Object c19f185fd70cefc696ba14 bject key, EventArgs e) reactive(EventArgs e, ToolStripItemEventType met) useEventArgs e, ToolSt	esponseStream, Bool , Byte[] data) ,fdb5bb8b44119a108 ia1ad8b8a8a5e57cca2 tiring attachmentID, f umentItem, String att. entFileName) I8af1c4faf54, EventAr	lean asyncCal :82f1a() 214a3)(c72dcf Byte[] data) achmentPath :gs cf1018bb8
etails	Se	end Error Report	Don't Send

Error Message Dialog

STEPS

- 1. Open the IIS Manager on the server where Devolutions Password Server is hosted.
- 2. Expand the **Tree View** and select the Devolutions Password Server web application name and open the **Configuration Editor** in the **Management** section.



3. Select the value *system.webServer/serverRuntime* in the **Section** drop down menu. Then, increase the value of the **uploadReadAheadSize** parameter. This value is in bytes so if you want to load a 50MB file, you have to change the value to 51200.

<i>6</i>]	Internet Inform	nation Services (IIS) Manager	_ D X	
VWINDSRV-DVLS	Sites Default Web Site dvlsg		🛛 🗠 🏠 🔞 •	
File View Help				
Connections	Section Section Editor	From: ApplicationHost.config <location default="" dvlsg'="" path="De Source Source</td><td>Actions Apply Cancel Generate Script Configuration Search Configuration</td></tr><tr><td>p — aspnet_client
p → aspnet_client
p → dvisg</td><td>client authenticatedUserOverride Use
enabled Tru
enableNagling Fals
frequentHitThreshold 22
frequentHitTimePeriod 00:
maxRequestEntityAllowed 429
uploadReadAheadSize 491</td><td>UseAuthenticatedUser
True
False
2
00:00:10
4294967295
49152</td><td>Section (Construction)
Revert To Parent
Unlock Section
(P) Help</td></tr><tr><td><<u> </u></td><td>uploadReadAheadSize
Data Type:uint
Value Range: Minimum:0 - Maximum:2,147,483,6</td><td>47</td><td></td></tr><tr><td>Configuration: ApplicationHost.config</td><td><location path=" site="" web=""></location>		€ <u>1.</u> ::

IIS Configuration Editor

For more information about these settings, you can consult this web page https://www.iis.net/configreference/system.webserver/server/net/net/configreference/system.webserver/server/server/net/configreference/system.webserver/server/server/net/configreference/system.webserver/server/server/net/configreference/system.webserver/serv

9.6.5 Failed Request Tracing with IIS

DESCRIPTION

This topic will present how to install and configure a **Failed Request Tracing Log** rule for troubleshooting HTTP 500 error issues on the IIS site.

• Enable Failed Request Tracing in IIS

A detailed step by step to add the role on a Windows Server 2012R2.

<u>Configure Failed Request Tracing</u>

Configuration needed for troubleshooting HTTP 500 error issues.

<u>Consult the Failed Request Tracing log</u>

Where and how to look at the Failed Request Tracing logs.

For more information about Failed Request Tracing, please visit https://www.iis.net/configreference/system.webserver/tracing/tracefailedrequests.

9.6.5.1 Enable Failed Request Tracing in IIS

ENABLE FAILED REQUESTS TRACING IN IIS



1. Open the Server Manager. Choose Add Roles and Features from the Manage menu.



Server Manager - Add Roles and Features

2. Select the Installation Type and then click Next.

A	Add Roles and F	eatures Wizard	_ D X
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and F type Select the installation type. You ca machine, or on an offline virtual ha Role-based or feature-based Configure a single server by add Remote Desktop Services ins Install required role services for or session-based desktop deplo	eatures Wizard VWINDSI In install roles and features on a running physi rd disk (VHD). installation ding roles, role services, and features. tallation Virtual Desktop Infrastructure (VDI) to create syment.	DESTINATION SERVER RV-RDMS2.windjammer.loc cal computer or virtual
		< Previous Next >	stall Cancel

Select Installation Type

3. Select the destination server and then click **Next**.

è	Add Roles and Features Wizard			
Select destination	DESTINATION SERVER DN SETVER VWINDSRV-RDMS2.windjammer.loc			
Before You Begin Select a server or a virtual hard disk on which to install roles and features. Installation Type Installation Type				
Server Selection Server Roles Features	Server Pool			
Results	Name IP Address Operating System VWINDSRV-RDMS2.win 192.168.7.23 Microsoft Windows Server 2012 R2 Datacenter			
	1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.			
	< Previous Next > Install Cancel			

Select Destination Server

4. On the Select server role page, expand the Web Server (IIS) role, expand Web Server and expand Health and Diagnostics. Then select Tracing and click Next.



Select Server Roles

5. On the page Select features, click Next.

L	Add Roles and Features Wizard	_ D X
Select features		DESTINATION SERVER VWINDSRV-RDMS2.windjammer.loc
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection	N NET Framework 3.5 Eastures (1 of 3 installed)	.NET Framework 3.5 combines the
Server Roles	INET Framework 4.5 Features (3 of 7 installed)	power of the .NET Framework 2.0
Features	▷ Background Intelligent Transfer Service (BITS)	building applications that offer
Confirmation	BitLocker Drive Encryption	appealing user interfaces, protect
Results	BitLocker Network Unlock	information, enable seamless and
	BranchCache	secure communication, and provide
	Client for NFS	the ability to model a range of
	Data Center Bridging	business processes.
	Direct Play	
	Enhanced Storage	
	Failover Clustering	
	Group Policy Management	
	IIS Hostable Web Core	
	Ink and Handwriting Services	
	· · · · · · · · · · · · · · · · · · ·	
	· · · · · · · · · · · · · · · · · · ·	
	< Previous Next	> Install Cancel

Select features

6. On the page **Confirm installation selections**, click **Install**.

Pa	Add Roles and Feature	s Wizard	_ 🗆 X
Confirm installati	Add Roles and Feature On selections To install the following roles, role services, Restart the destination server automat Optional features (such as administration t been selected automatically. If you do not their check boxes. Web Server (IIS) Web Server Health and Diagnostics Tracing	s Wizard vwindsf or features on selected server, click In tically if required ools) might be displayed on this page want to install these optional features	DESTINATION SERVER RV-RDMS2.windjammer.loc istall. because they have i, click Previous to clear
	Export configuration settings Specify an alternate source path		
	<	Previous Next >	istall Cancel

Confirm Installation selections

7. On the **Results** page, click **Close**.



9.6.5.2 Configure Failed Request Tracing

CONFIGURE FAILED REQUESTS TRACING



1. In the Server Manager, click on the Tools menu and open the Internet Information Services (IIS) Manager.



2. In the **IIS Manager**, expand the **Web site (VWINDSRV-RDMS2)**, expand **Sites** and then select **Default Web Sites**.



Internet Information Services (IIS) Manager

3. On the right, in the Actions pane, select Failed Requests Tracing....

Act	ions
6	Explore
	Edit Permissions
	Edit Site
	Bindings
	Basic Settings
	View Applications
	View Virtual Directories
Ma	nage Website
2	Restart
₽	Start
	Stop
	Browse Website
0	Browse *:80 (http)
	Advanced Settings
	Configure
E	Failed Request Tracing
	Limits
9	Install Application From Gallery
?	Help
	Actions Pane

- 4. Select the **Enable** check box and then click **OK**. The Directory target and the Maximum number of trace files can be modified.

Edit Website Failed Request Tracing Settings ? ×
✓ Enable
Directory:
%SystemDrive%\inetpub\logs\FailedReqLogFiles
Maximum number of trace files:
50
OK Cancel

Edit Website Failed Request Tracing Settings



5. Expand **Default Web Site** and select the Web site to be traced.

6. Double click on the Failed Request Tracing Rules icon of the selected Web Site.



Internet Information Services (IIS) Manager

7. In the Actions pane on the right, click on Add... to add a new rule.

9	Internet Info	rmation Services (IIS)	Manager	_ □ X			
€ VWINDSRV-RDMS2 ► Sites	🐱 🛛 🏠 🔞 🗸						
File View Help							
Connections	Failed Use this feature to logged either wher taken for the reque been fulfilled, the f Group by: No Gri	Request Tracing configure tracing for faile an error status code is gy est exceeds a specified dur irst condition that is met ouping	J Rules d requests. A request trace is enerated or when the time ation. If both conditions have will generate the request trace.	Actions Add Revert To Parent View Ordered List P Help			
 ▷-[a aspnet_client ▷-[b aspnet_clie	Path •	Associated Provid	Status Codes				

Failed Request Tracing Rules

8. Select ASP.NET (*.aspx) and click Next.

Add Failed Request Tracing Rule	?	x
Specify Content to Trace		
What would you like to trace? All content (*) ASP.NET (*.aspx) ASP (*.asp) Custom: Example: tr*.aspx		
Previous Next Finish	Cancel	

Specify Content to Trace

9. Select the **Status Code(s)** check box. Enter the type of the status code to be traced, in this case type in the **status code 500**, and click **Next**.

	Add Failed Reques	t Tracing Rule		? X
Define Trace Con	ditions			
Under which condition(s) sho	ld a request be traced?			
 ✓ Status code(s): 500 Example: 401.3-999,405 				
Time taken (in seconds):				
Event severity: Error	¥			
	Previous	Next	Finish	Cancel

Define Trace Conditions

10. The last setting is to select the providers of the tracing. Select **ASPNET** and **WWW** Server. For each of them, set the **Verbosity** to **Verbose**. Finally, check all Areas settings for these two providers and click **Finish**.

	Add Failed Request Tracing Rule ? X
Select Trace Providers	5
Providers:	Provider Properties Verbosity: Verbose Areas: Authentication Aces: Authentication Security Filter StaticFile CGI Compression Cache RequestNotifications Module

Select Trace Providers

11. The tracing rule is now defined.



9.6.5.3 Consult the Failed Request Tracing log

CONSULT THE FAILED REQUEST TRACING LOG

With **Failed Request Tracing enabled**, the logs files are created and populated in the directory set up on step <u>Edit Website Failed Request Tracing Settings</u>. By default, the path is **%SystemDrive%\inetpub\logs\FailedReqLogFiles**. In this place, a folder typically named **W3SVC1** will be created when the first case happen.

There will be an XSL file (freb.xsl) for the display style in an XML viewer like Internet Explorer. Also, the most important, the XML files (fr#######.xml). Open an XML file to view the log triggered by the tracing rule.



Here is an example of a Failed Request Tracing log:

					- 🗆 X
🗧) 🔿 📳 C:\inetpub\logs\Faile	dReqLogFiles\W3SVC1\fr0000	♀ ♂ 🖉 vwind	dsrv-rdms2 ×		📅 🖈 🕸
Request Diagnostics for GET I	http://vwindsrv-rdms2:80	/DS5/test:test			
Request Request Summary Details	Compact View				
– Request Summary					
Url http://vwi	ndsrv-rdms2:80/DS5/test:te	est	Site	1	
App Pool DS5			Process	5812	
Authentication NOT_AVAI	LABLE		Failure Reason	STATUS_CODE	
User from token			Trigger Status	400	
Activity ID {8000031	5-0000-EB00-B63F-84710C	7967BB}	Final Status	400	
			Time Taken	969 msec	
- Errors & Warnings	Event		Module Name		
69. view Warning	- MODULE_SET_RESPO	NSE_ERROR_STAT	ASPxHttpHandler	Module	
trace	ModuleName ASF Notification BEC HttpStatus 400 HttpReason Bad HttpSubStatus 0 ErrorCode The Uly (0)	PxHttpHandlerModul SIN_REQUEST I Request coperation complete co)	e ed successf		
See all events for the reques	ConfigExceptionInfo t				

Failed Request Tracing log

9.6.6 IIS Logging

DESCRIPTION

Here is the description of desired settings when we troubleshoot a performance/connectivity issue related to the client application.

IIS WEB SITE LOGGING

1. Open **IIS Manager** and go in the **Logging** settings.



IIS Manager

2. Click on Select Fields

V	Internet Information Services (IIS) Manager		- 🗆 🗙
	Sites → Default Web Site →		😰 🛛 🟠 🔞 🗸
File View Help			
Connections	Use this feature to configure how IIS logs requests on the Web server. One log file per: Site	^	Actions Apply Cancel Disable View Log Files Help
-	Log File Format: W3C Directory: %SystemDrive%icetpub\logs\LogFiles Encoding: UTF-8 UTF-8 Log Event Destination Select the destination where IIS will write log events. © Log file only CTW event only © Both log file and ETW event		
	Log File Rollover Select the method that IIS uses to create a new log file. Schedule: Daily Maximum file size (in bytes): <	*	
< >	E Features View		
Configuration: 'localhost' application	Host.config , <location path="Default Web Site"></location>		· · · · · · · · · · · · · · · · · · ·

Logging Panel

3. We recommend that at the very least the following fields be selected:



Field selection Dialog

APPLICATION POOL RECYCLE

The application pool that is in fact running the instance can be restarted for a multitude of reasons. It may be useful to know when those **recycles** occur as well as the reasons. Go in the **Application pools** section of the **IIS manager**, then open the **Advanced settings** for your application pool. Enable all of the **Recycle events**, it will create a log entry in the **Windows Event Log**.



Advanced settings for an Application Pool.

9.6.7 The remote server returned an error: (400) Bad Request

DESCRIPTION

You get the following Error message dialog when you try to authenticate on the Devolutions Password Server instance with Remote Desktop Manager.
Remote Desktop Manager
Unable to Connect to your Data Source
DVL5 server is not responding. The remote server returned an error: (400) Bad Request. Message
Devolutions. RemoteDesktopManager: Business. TryGoOfflineException: DNL5 server is not responding. The remote server returned an error: (400) Bad Request: at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSConnectionDataSource. c6b670699089bd1:9688221883b0c338f(String c18973cea236a9feff75c32ca7d1697d5, String ceb81d1ee93f91e0bc57f34876c263863, Boolean c1 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSConnectionDataSource. c6b870699089bd1:9688221883b0c338f(String c18973cea236a9feff75c32ca7d1697d5, String ceb81d1ee93f91e0bc57f34876c263863, Boolean c1 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSConnectionDataSource. c8b87b6ce23693(String c18973cea236a9feff75c32ca7d1697d5, String ceb81d1ee93f91e0bc57f34876c263863, Boolean c1 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSConnectionDataSource. c680870498b3ae30aad5318fa57dc6159, String ceb81d1ee93f91e0bc57f34876c263863, Boolean c1 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSConnectionDataSource. c68087049691a26117253e0 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c51e362c2cae20ee3255558da7e96d5882c3e80844d2f0H1fff093ae0667a3199fb() at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c51e362c2cae20eea95558da7e96d5882c36418a1d808886557ccae14a3(31561c0d54939abd223ac70cf30e7e6^11c6cc9ab02b2ea9ccd42c7c0497 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c6546fc72005500dd94253acf30D6d10H1ff093ae0667a3199fb() at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c6546fc72005500dd94253acf30D6d10H1ff093ae0667a3199fb() at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c6546fc72005500dd94253475010b40323ac70cf30e7e6^11c6cc9ab02b2ea9ccd42c7c0497 at Devolutions. RemoteDesktopManager. Business. DataSources. RDMSVebApcillent. c6546fc7200564004978504b30076658b2285781) at Devolutions. RemoteDesktopManager. Rusiness. ContextinnManager. c24954db4300rd
OK

Error message Dialog

SOLUTION

There are two different solutions for this issue.

- 1. Reduce the number of AD Groups that the user account is part of. We are aware that most of the time, because of the design of the AD structure, it is not possible to reduce the number of AD groups.
- Increase the settings for the MaxFieldLength and the MaxRequestBytes registry entries on the server. Please consult the following Microsoft article for more information on how to increse these values. <u>https://support.microsoft.com/enus/help/2020943/http-400-bad-request-request-header-too-long-response-to-httprequest</u>

9.6.8 The remote server returned an error (405) Method Not Allowed

DESCRIPTION

You get the following Error message dialog when you try to create or modify an entry.

📮 Remote Desktop Manager		×
Error message dialog	J	
The remote server returned an error: (405)	Method Not Allowed.	
Enterprise Edition 12.0.8.0	Memory usage: 869 MB	
Running since: 7 hours 35 min 48 sec	WebException	
Message		
at System.Net.HttpWebRequest.GetResponse() at Devolutions.Server.ApiWrapper.RestClient.Pu at Devolutions.Server.ApiWrapper.RestClient.Pu at Devolutions.RemoteDesktopManager.Busines at Devolutions.RemoteDesktopManager.Busines at Devolutions.RemoteDesktopManager.Busines at Devolutions.RemoteDesktopManager.Busines at Devolutions.RemoteDesktopManager.Manag at Devolutions.RemoteDesktopManager.Manag at Devolutions.RemoteDesktopManager.Manag at Devolutions.RemoteDesktopManager.Manag at Devolutions.RemoteDesktopManager.Manag at Devolutions.RemoteDesktopManager.Manag at System.Windows.Forms.ToolStripItem.Handle at System.Windows.Forms.ToolStripItem.Handle at System.Windows.Forms.ToolStripItem.FireEv at System.Windows.Forms.ToolStripItem.FireEv at System.Windows.Forms.ToolStripItem.Perfor at Devolutions.RemoteDesktopManager.Frames	tRequest[T, U](String apiUrl, T putObject) ent.SaveConnection(ConnectionInfoEntity connectionInfo) is.DataSources.RDMSWebApiClient.c4cfebae48c715cba5241d6 is.DataSources.RDMSWebApiClient.c4ffebae48c715cba5241d6 is.DataSources.RDMSWebApiClient.c4ffebc72c053c0cd60a62at is.DataSources.RDMSWebApiClient.c4ffebc72c053c0cd60a62at is.DataSources.RDMSWebApiClient.c4ffebc72c053c0cd50a293 is.DataSources.RDMSWebApiClient.c4ffebc72c053c0cd50a293 is.DataSources.RDMSWebApiClient.c4ffebc72c053c0cd50a293 is.ConnectionManager.c1d62rcc9d0263a9358aca9abc885 ers.ConnectionManager.c1d62rcc9d026a39358aca9abc885 ers.SessionMenuManager.cd94813672b0ecea85dc17deccf3b30 vent(Object key, EventArgs e) Diclick(EventArgs e) Click(EventArgs e) Click(EventArgs e, ToolStripItemEventType met) ent[EventArgs e, ToolStripItemEventType met) mClick() .FreDashBoardBase.ButtonOnClick(Object sender, EventArgs e	3b026a1ca.c862ffa26b23a5a73cecc6142fe84c070() a671d47c8d[cb75a0a5d15a1ad8b8a8a5e57cca214a3](c31561c0d54939a innectionInfo connection) Connection connection) b(Connection c6ae3d31dfb3fea36c5f53f7fe93584c, BaseConnection a5ource connectionDataSource, Connection connection, Connectior 9) 7e(Object c19f185fd70cefc696ba148af1c4faf54, EventArgs cf1018bb8

Error message Dialog

STEPS

Please note that you will have to restart the server after removing the WebDAV Publishing role to complete the procedure.

- 1. On the server where the Devolutions Password Server instance is hosted, open the **Server Manager** application.
- 2. Then, open the **Remove Roles and Features** in the **Manage** menu.

a	Server Manager				
🔵 🗧 👊 Dashb	oard	• 🅄 🚩 Manage	Tools View Help		
		Add Roles and Features			
		Remove Roles and Features	<u>^</u>		
Dashboard	WELCOME TO SERVER	Add Servers			
Local Server		Create Server Group			
All Servers		Server Manager Properties	server		
File and Storage Services D			berver		
Server Manager					



3. In the Server Roles, uncheck the WebDAV Publishing role.

Remove Roles and Features Wizard Dialog

4. Click on the **Remove** button to uninstall the WebDAV Publishing role from the server.

L	Remove Roles and Features Wizard	_ D X
Confirm removal Before You Begin Server Selection Server Roles Features Confirmation Results	Remove Roles and Features Wizard selections To remove the following roles, role services, or features from the Restart the destination server automatically if required Web Server (IIS) Web Server Common HTTP Features WebDAV Publishing	DESTINATION SERVER QA-VDOWNDVLS.downhill.loc
	< Previous Next >	Remove

Remove Roles and Features Wizard Dialog

9.6.9 The encryption file is missing

DESCRIPTION

When opening the Devolutions Password Server web interface, the error The encryption file is missing, please contact your administrator is displayed.



Devolutions Password Server login page

This issue is the result of using an old version of Remote Desktop Manager Enterprise Edition for Windows (prior to version 13.0.x.x) to install Devolutions Password Server version 4.7.x.x.

SOLUTION

Install Remote Desktop Manager Enterprise Edition for Windows version 13.0.6.0 or higher and then reinstall Devolutions Password Server version 4.7.1.0 or higher over the current instance with the **Upgrade Server** button.

9.6.10 The INSERT statement conflicted with the FOREIGN KEY constraint "FK_ConnectionState_ConnectionID"

DESCRIPTION

As an administrator of the Devolutions Password Server instance, you receive this error message.

Error:

SqlException - The INSERT statement conflicted with the FOREIGN KEY constraint "FK_ConnectionState_ConnectionID". The conflict occurred in database "DVLS", table "dbo.Connections", column 'ID'. The statement has been terminated. at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) at System.Data.SglClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) at System.Data.SglClient.TdsParser.TryRun(RunBehavior runBehavior, SglCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) at System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption) at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean describeParameterEncryptionRequest) at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean inRetry) at System.Data.SglClient.SglCommand.InternalExecuteNonQuery(TaskCompletionSource 1 completion, String methodName, Boolean sendToPipe, Int32 timeout, Boolean& usedCache, Boolean asyncWrite, Boolean inRetry) at System.Data.SqlClient.SqlCommand.ExecuteNonQuery() at Devolutions.Server.DatabaseManager.ExecuteNonQuery(String sql, IEnumerable`1 parameters, CommandType commandType) at Devolutions.Server.ConnectionLogManager.AddLogEntry(SessionContext context, LogEntryEntity logEntry) --- INSERT INTO ConnectionLog ([ID],[Username], [MachineName], [Message], [MessageType], [ConnectionName], [ConnectionTypeName], [ConnectionID], [ConnectionUserName], [StartDateTime], [EndDateTime], [StartDateTimeUTC], [EndDateTimeUTC], [GroupName], [CustomerID], [Comment], [LoggedUserName], [Prompt], [SecurityGroup], [Cost], [Data], [UserInfoID], [SupportClose], [CloseMode], [OpenMode], [HostName], (?,?,?,?,?,?,?,?,?,?,?,?,?,?)

Please contact us at <u>ticket@devolutions.net</u> and we will send you a SQL statement to execute on the database to fix this issue.

Contents	583
----------	-----

Index

- H -

high availability 14

- L -

LDAPS 518 licence license renew key 540 load balancing 14

- 0 -

on-premise on-premises 10 optimize 88

- T -

topology 14



Control the IT Chaos

Contact Us

For any questions, feel free to contact us: Support: support@devolutions.net Skype: support.devolutions Phone: +1 844 463.0419 Monday to Friday 8 a.m. to 4 p.m. EST

Head Office Devolutions inc.

1000 Notre-Dame Lavaltrie, QC J5T 1M1 Canada