

Der PiSA sales Web-Client

Anwendung, Installation und Konfiguration

Release: V.7

Stand: 10/2020

Dok.-Nr: D-16-167574, V5

Erstellt durch: PiSA sales GmbH
D-14050 Berlin, Fredericiastraße 17-19
Tel.: + 49 (0)30/81 07 00 – 00
Fax.: + 49 (0)30/81 07 00 – 99
E-Mail: info@pisasales.de

Inhalt

1. Der PiSA sales Web-Client	4
1.1 Zu diesem Dokument.....	4
1.2 Einsatzempfehlungen für den PiSA sales Web-Client.....	4
1.3 Vom Windows-Client abweichende Features	4
1.4 Desktop-Integration/Kopplungen.....	5
1.5 Systemarchitektur	8
1.6 Systemvoraussetzungen.....	9
2. Installation und Konfiguration des Web-Servers.....	10
2.1 Web-Server-Maschine bereitstellen	10
2.2 Web-Server installieren	10
2.3 Web-Server vorbereiten	10
2.3.1 Arbeitsverzeichnis festlegen	10
2.3.2 Zugriff auf das Administrations-Servlet einrichten	10
2.3.3 Session Timeout einstellen.....	12
2.4 Web-Client WAR installieren/hochladen (Deployment).....	13
3. PiSA sales Web-Client™ konfigurieren.....	14
3.1 Umgebungsvariablen des PiSA sales Web Client™	15
3.2 Einstellungen am PiSA sales Applikationsserver, die den Web-Client beeinflussen	17
4. Konfiguration der Login Sets	18
4.1 OpenID Connect (OAuth2) für den Web-Client (erst mit 7.6 im Standard).....	19
4.1.1 Vereinfachter Ablauf einer OpenID Connect Authentifizierung	19
4.1.2 Voraussetzungen.....	20
OpenID Connect (OAuth2) Einrichtung am Web-Client	21
4.1.3 Nutzung des Discovery-Dokuments	21
Behandlung von OpenID Connect im Server.....	22
4.1.4 Umfang der OpenID Connect Authentifizierungsinformationen	23
4.1.5 OpenID-Konfiguration	24
4.1.6 OpenID-Benutzer	24
5. Benutzer-Login.....	25
5.1 URL-Parameter	25
5.2 Installation der PiSA sales Desktop-Integration.....	26
5.2.1 Installationsvoraussetzungen.....	26
5.2.2 Desktop-Integration installieren:	26
5.2.3 PiSA sales Desktopintegration (DIM) im Browser zulassen.....	28
6. Portable Web-Client-Anwendung.....	30

1. Der PiSA sales Web-Client

1.1 Zu diesem Dokument

Das Dokument gibt Empfehlungen für den Einsatz des PiSA sales Web-Client und beschreibt technische Voraussetzungen, Installation und Konfiguration des PiSA sales Web-Applikationsservers.

1.2 Einsatzempfehlungen für den PiSA sales Web-Client

Der PiSA sales Web-Client ermöglicht Benutzern den Zugriff auf PiSA sales-Applikationen über den Internet-Browser. Er bietet – von wenigen Ausnahmen abgesehen – den gleichen Funktionsumfang wie der Windows-Client. Wir empfehlen, den Web-Client für folgende Benutzergruppen und in folgenden Szenarien einzusetzen:

- + Mitarbeiter im Homeoffice ohne VPN-Zugang
- + Vertriebspartner, Lieferanten, OEM-Partner, Händler, Kunden mit speziellen Sichten auf den CRM-Datenbestand und/oder eingeschränktem Funktionsumfang, z.B. Anfrageportal, Projektinformationsportal
- + Benutzergruppen, die nicht Windows als Betriebssystem nutzen (z.B. Mac OS oder Linux) und somit keinen Windows-Client installieren können
- + Benutzergruppen, die Tablets mit Tastatur benutzen (z.B. Windows Surface)
- + Portal-Anwendung mit vom Standard abweichenden Masken, Funktionen und Workflows
- + Zugriff für externe Kontakte oder Gast-User auf Fragebögen/Formulare zur Erfassung von Daten, die im CRM-System personalisiert oder anonymisiert gespeichert werden sollen

1.3 Vom Windows-Client abweichende Features

Zusätzliche Features:

- + Der Web-Client bietet als Weiterentwicklung des Entry Portals einen persönlichen Kalender mit Tages-, Wochen- und Monatsansicht. Mit dem Kalender können Sie so arbeiten wie in Groupware-Clients. Dieser Kalender steht im Windows-Client nicht zur Verfügung.

Gesperrte Features und Einschränkungen in V6.:

- + Einschränkungen beim interaktiven Skalieren und Dimensionieren von Masken
- + Einschränkungen bei der Unterstützung von Keyboard-Shortcuts

1.4 Desktop-Integration/Kopplungen

Für Office- und Groupware-Kommunikation des PiSA sales Web-Client wird die PiSA sales Desktop Integration als Schnittstelle eingesetzt, die alle zurzeit verfügbaren erforderlichen AddIns mitbringt. Sie ermöglicht unter anderem das Bearbeiten von Dokumenten direkt aus PiSA sales heraus, das Ein-/Auschecken von Dokumenten oder auch das Einchecken von E-Mails aus der Groupware.

Hinweise zur Installation siehe hier: [Installation der PiSA sales Desktop-Integration](#)

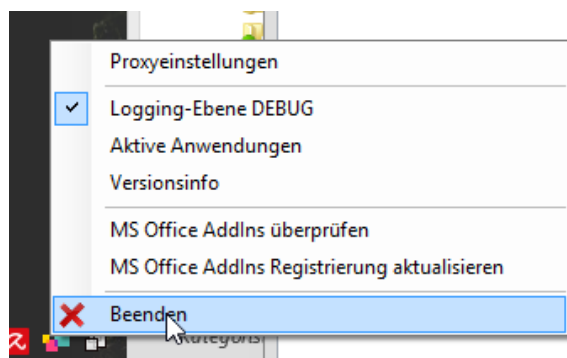
- + Dateihandling und Bearbeitung (z.B. Dokumente ein/auschecken, Dokumente in der verbundenen Anwendung, Snapshot im Dateisystem speichern)
- + Ab DIM 7.4.4.152 02/2019 Live Analyse, ob es rund um installierte oder notwendige Office AddIns, VSTO etc. Probleme gibt (z.B. eine Office 64-Bit-Version ohne VSTO).
- + MS Office-Kopplung zur Bearbeitung von Office-Dokumenten
- + Clientseitige Synchronisation von E-Mails und Kontakten mit MS Outlook
- + CTI-Kopplung
- + Für Analyse und Fehlersuche kann ein Debug-Logging an der DIM geschaltet werden.

Log-Level der Desktop-Integration dauerhaft auf ein bestimmtes Level schalten

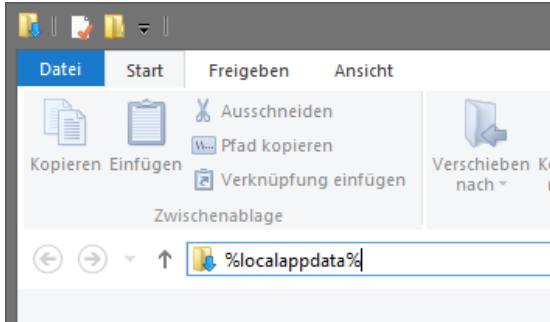
Um bei Problemen mit der Desktop-Integration ein Debug-Log-File zu schreiben, ist die Konfigurationsdatei der DIM anzupassen. Das Log-File, welches nun bei der Arbeit mit dem Web-Client die Debug-Informationen protokolliert, ist zu sichern, sobald ein Fehler auftritt, und dem PiSA sales-Support zuzusenden.

Gehen Sie bitte folgendermaßen vor:

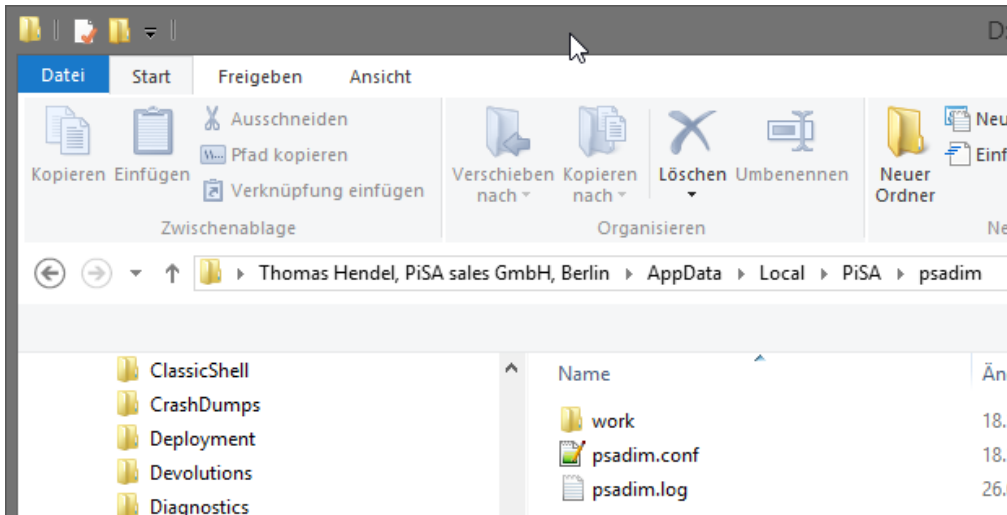
1. Loggen Sie sich am Web-Client aus, und beenden Sie die Desktop Integration.



2. Öffnen Sie ein Windows-Explorer-Fenster und tragen Sie „%localappdata%“ in die Adress-/Ordner-Zeile ein (ohne Quotes).

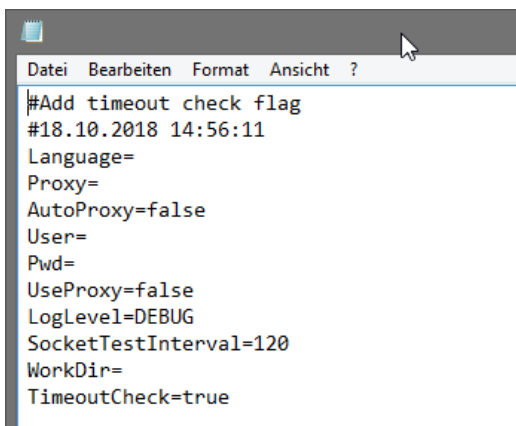


Mit [Enter] wechselt der Explorer in den entsprechenden Ordner. Hier finden Sie den Unterordner [PiSA], darin den Unterordner [psadim], die Sie bitte jeweils öffnen (Doppelklick).



3. Die Datei „psadim.conf“ in dem Ordner [psadim] müssen Sie nun zum Bearbeiten öffnen (Rechtsklick / „Öffnen mit...“ und Editor auswählen bzw. „Bearbeiten“).

So könnte die Konfiguration aussehen:



4. In der Zeile „LogLevel=“ steht normalerweise der Parameter INFO. Ändern Sie diesen Eintrag wie im Bild in DEBUG. Speichern Sie die Konfigurationsdatei.
5. Beenden Sie die Bearbeitung, rufen Sie den Web-Client auf (dabei wird die Desktop Integration gleich wieder gestartet) und loggen Sie sich in PiSA sales ein.

Die Datei „psadim.log“ in dem Ordner [psadim] wird nun größer, weil umfangreiche Debug-Informationen protokolliert werden.

ACHTUNG: Die Datei wird bei jedem Start der Desktop-Integration – also im Normalfall beim Anmelden des Benutzers – überschrieben!

Daher ist es wichtig, sobald ein Fehler auftritt, das Log-File für eine Analyse zu sichern!

- Sofort alle Web-Client-Sitzungen beenden (Ausloggen),
- die Desktop Integration wie oben beenden,
- in den Ordner [psadim] wechseln,
- die Datei „psadim.log“ lokal sichern oder zumindest umbenennen,
- die Datei dem PiSA sales-Support zusenden.

Danach kann wieder normal mit dem Web-Client weitergearbeitet werden. Solange das DEBUG-Level in der Konfigurationsdatei eingetragen ist, werden alle Informationen weiter im Log-File protokolliert.

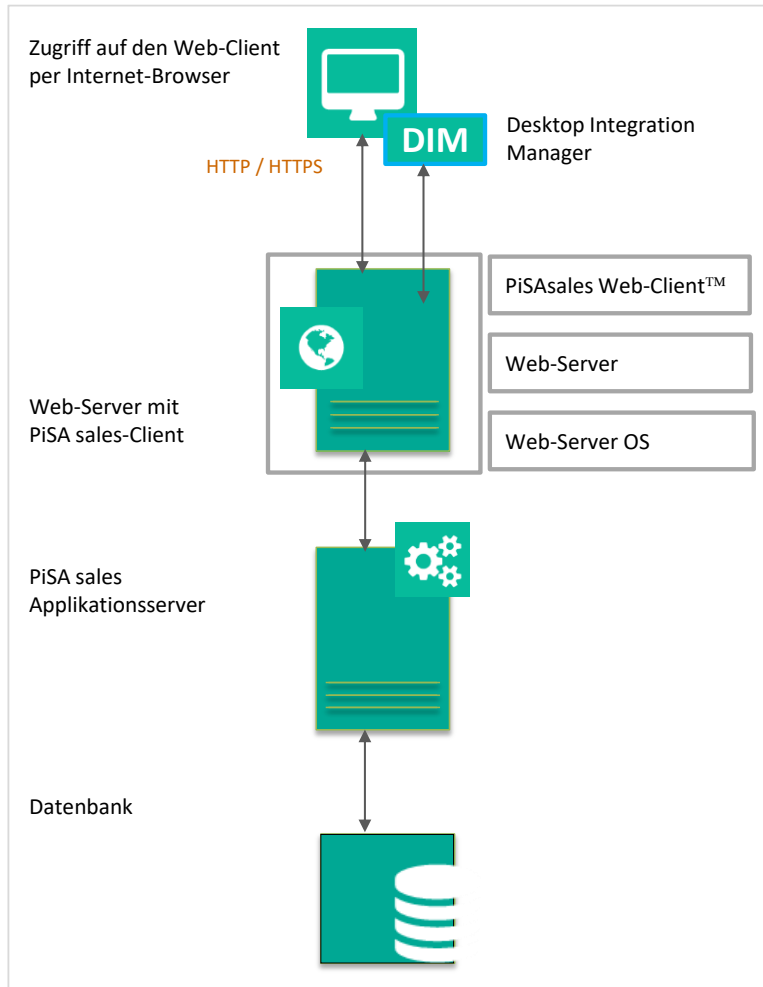
HINWEIS:

Neben der beschriebenen „sicheren“ Methode können Sie die Desktop Integration auch alternativ einfach beenden, ohne sich auszuloggen.

ACHTUNG: Dann wird der Web-Client eine Warnmeldung anzeigen – die Sie aber **erst** bestätigen dürfen, wenn Sie die Log-Datei gesichert bzw. umbenannt haben.

Andernfalls startet die Desktop-Integration einfach neu und überschreibt alle Protokolleinträge im Log-File.

1.5 Systemarchitektur



HINWEIS: Die Desktop-Integration ist nicht dringend notwendig, um Basisfunktionalitäten des Web Clients zu verwenden (Portal-Modus). Um eine Kopplung des Web Clients zu Office Anwendungen und bessere Zugriffsmöglichkeiten auf das Dateisystem des Clients zu gewährleisten, wird die Installation der Desktop-Integration jedoch erforderlich.

1.6 Systemvoraussetzungen

PiSA sales Web-Applikationsserver:

- + Web Server OS: Windows oder Linux
- + Web-Server: Apache Tomcat 8; Oracle WebLogic (10.3 +); JBoss AS 6; Eclipse Virgo (2.1+)
- + Speicherbedarf 40 MB pro Applikation zuzüglich ca. 10 MB pro eingeloggtem Benutzer
- + Java virtual machine (JVM) 8 oder höher
- + Offene http- oder https-Ports für den Zugriff auf den Web-Applikationsserver
- + Offener Port (28000) für den Zugriff auf den PiSA sales Applikationsserver
(Tomcat <->PiSA sales, nicht nach außen)

PiSA sales Web-Client (Internet-Browser)

- + Unterstützte Browser: Firefox aktuelle Versionen, Chrome und weitere Webkit-basierte Browser wie Opera/Vivaldi, Edge, IE ab V11
- + Der Einsatz des IE wird allerdings nicht empfohlen. Die Performance ist geringer und die Fehleranfälligkeit ist höher als bei anderen Browsern.
- + Grafikauflösung ab 1024x786 Pixel

2. Installation und Konfiguration des Web-Servers

2.1 Web-Server-Maschine bereitstellen

1. Web-Server-Maschine bereitstellen. Die Maschine muss je nach Anwendungsfall von außen oder im internen Unternehmensnetzwerk erreichbar sein.
2. Java-Umgebung installieren, falls dies nicht Bestandteil der Web-Server-Installation ist (wie z.B. bei Oracle WebLogic Server).

2.2 Web-Server installieren

1. Web-Applikationsserver installieren.
2. Zugriff auf Web-Applikationsserver einrichten (Zertifikate für https, Ports für https)

2.3 Web-Server vorbereiten

Der PiSA sales Web Client™ wird als WAR-Datei bereitgestellt und muss auf dem Web-Server bereitgestellt werden. Es können mehrere Instanzen des PiSA sales Web Client™ installiert werden. Bevor ein die Bereitstellung erfolgen kann, muss der Web-Server vorbereitet werden. Dies umfasst drei Schritte:

1. Arbeitsverzeichnis konfigurieren
2. Zugriff auf Administrations-Servlets einrichten
3. Session-Timeout einstellen

2.3.1 Arbeitsverzeichnis festlegen

Im Arbeitsverzeichnis werden Login-Sets, benutzerspezifische Anwendungseinstellungen, konvertierte BLOBS (Binary Large Objects z.B. .ico -> .png) und temporäre Dateien gespeichert. Der Verzeichnispfad wird in der Betriebssystem-Umgebungsvariable PSCWEBCLI_WORK angegeben. Stellen Sie sicher, dass der Pfad existiert und dass der Benutzer, der die Web Server-Anwendung startet/ausführt, Schreibenden Zugriff auf das Verzeichnis hat. Ist kein spezielles Arbeitsverzeichnis konfiguriert, wird \${USER_HOME}/.pscwebcli verwendet. Existiert dieses Verzeichnis nicht, wird das Root-Verzeichnis des Web-Servers \${ROOT}/.pscwebcli genutzt. Jedoch nur dann, wenn dies der Web-Server mit seinen (meist strengen) Zugriffsbeschränkungen auf Stammverzeichnisse zulässt.

Empfehlung: Wir empfehlen, den Verzeichnispfad grundsätzlich zu setzen, damit mögliche Fehlerquellen erst gar nicht aufkommen.

2.3.2 Zugriff auf das Administrations-Servlet einrichten

Der PiSA sales Web Client™ inkludiert zwei Servlets, ein Benutzer-Servlet für den Zugriff durch Standard-Benutzer und ein Administrator-Servlet für den Zugriff durch Administratoren. Administratoren können Login-Sets für Standard-Benutzer anlegen und mit Hilfe von

Umgebungsvariablen den PiSA sales Web Client™ konfigurieren. Das Administrator-Servlet akzeptiert folgende Rollen: *pisaadmin*; *admin*, *manager -gui*.

Die Admin-Rolle ist in der Regel im Web-Server vorkonfiguriert. Wollen Sie auch Standard-Benutzern Administratorrechte geben, wird empfohlen, zusätzlich die *pisaadmin*-Rolle anzulegen und den Benutzern zuzuweisen.

HINWEIS für WebLogic-Server: Die WebLogic Konfiguration weicht vom Standard JEE ab. Deswegen muss man für WebLogic immer einen *pisaadmin* Benutzer anlegen.

pisaadmin-Rolle für Apache Tomcat einrichten

1. Navigieren Sie zum Verzeichnis `${TOMCAT_HOME}/conf`
2. Öffnen Sie die Datei *tomcat-users.xml* in einem Editor. Die Datei enthält eine Liste der Tomcat-User. Jeder User hat einen Eintrag in folgender Form:

```
<user name="..." password="..." roles="..." />
```

3. Identifizieren Sie den User, dem Sie die *pisaadmin*-Rolle zuordnen wollen. Nehmen Sie ggf. einen neuen User in die Liste auf. Das *roles*-Attribut ist ein kommaseparierter String von Rollen. Fügen Sie dem String den Wert *pisaadmin* hinzu.

pisaadmin-Rolle (principal) für Oracle WebLogic einrichten

1. Starten Sie die Oracle WebLogic Admin-Konsole. Sie wird aufgerufen mit:

```
http://<host>:7001/console
```

2. Melden Sie sich als Administrator oder principal an, der das Recht hat Sicherheits-Einstellungen zu modifizieren.
3. Navigieren Sie zur Security configuration section und wählen Sie Security Realms.
4. Selektieren Sie den Bereich, der den *PiSA sales Web Client* hosten wird.
5. Wählen Sie im Konfigurations-Dialog den Reiter *Users and Groups*. Er zeigt die Liste aller User des Bereichs.
6. Wählen Sie *Neu* und tragen Sie die geforderten Informationen ein:

Name:	<i>pisaadmin</i>
Description:	PiSA Web Client Administrator
Provider:	DefaultAuthenticator
Password:	<Bitte ein sicheres Passwort wählen!>

7. Bestätigen Sie mit OK. Der neue *pisaadmin*-User sollte nun in der Bereichs-User-Liste enthalten sein.
8. Jetzt können Sie den *PiSA sales Web Client™* verwenden. Sie erhalten Zugriff auf die Administrations-Konsole unter `<contextroot>/pisaadmin`.

2.3.3 Session Timeout einstellen

Der PiSA sales Web Client™ unterstützt mithilfe der Umgebungsvariable *SSN_ALV_TIM_OUT* (Siehe Kap.3) das Setzen eines Session-Timeout in Minuten. Dabei handelt es sich um ein Mindest-Intervall zwischen zwei aufeinander folgenden Pings vom Client (Browser) auf den Web-Server (z.B. Tomcat). Mit diesen Pings wird überwacht, ob die Anwendung noch aktiv ist oder bereits beendet wurde (z.B. durch Logout oder Schließen des Browser-Tabs/Fensters).

Das Timeout des PiSA sales Web Client™ muss kleiner sein als das globale Session-Timeout des Web-Servers. Wir empfehlen als Wert die Hälfte des globalen Web-Server-Session-Timeouts einzutragen. Ist der Wert für die praktische Anwendung zu klein, sollten Sie das globale Web-Server-Timeout erhöhen.

Globales Session-Timeout für Apache Tomcat ermitteln/einstellen

1. Navigieren Sie zum Verzeichnis `${TOMCAT_HOME}/conf`
2. Öffnen Sie die Datei `web.xml` in einem Editor.
3. Die Session-Timeout-Einstellungen finden Sie zwischen den Servlet-Mappings und den MIME-Type-Mappings. Der Wert ist in Minuten angegeben. Standard ist 30min.

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

4. Ändern Sie den Wert und starten Sie den Web-Server neu.

Globales Session-Timeout für Oracle WebLogic ermitteln/einstellen

1. Starten Sie die Oracle WebLogic Admin-Konsole. Sie wird aufgerufen mit:

```
http://<host>:7001/console
```

2. Melden Sie sich als Administrator oder principal an, der das Recht hat, die Server-Umgebung zu modifizieren.
3. Navigieren Sie zur *Environment section* und wählen Sie *Server*. Es wird eine Liste aller WebLogic Server Instanzen angezeigt.
4. Ändern Sie das Timeout für alle Server-Instanzen, die den PiSA sales Web Client™ hosten. Das geht wie folgt:
5. Öffnen Sie den Konfigurations-Dialog durch Klick auf den Server-Namen.
6. Navigieren Sie in den Reiter *Configuration -> Overload*. In der Konfigurationsliste sehen Sie den Eintrag *Maximum time for hanging threads*. Der Wert ist in Sekunden angegeben. Standard ist 600sec.
7. Ändern Sie den Wert, speichern Sie die Konfiguration und starten Sie den Web-Server neu.

2.4 Web-Client WAR installieren/hochladen (Deployment)

Stellen Sie den von PiSA sales gelieferten Web-Client (WAR-Datei) mit Hilfe der Manager-Konsole des Web-Servers bereit (Deployment).

HINWEIS: Hinweise zur Bereitstellung von Anwendungen finden Sie in der Web-Server-Dokumentation.

Beispielhaftes Deployment auf Apache Tomcat:

1. Rufen Sie im Browser die URL-Adresse des Tomcat-Managers auf.

`http(s)://host:8080/manager/html`

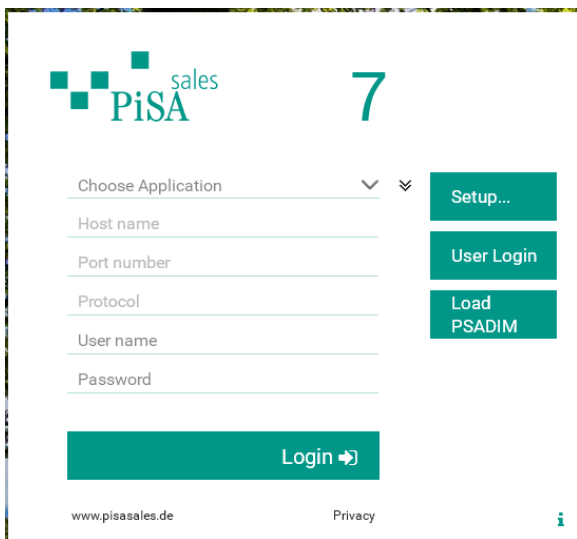
2. Wählen Sie im Bereich *Deploy* -> *War file to deploy* das WAR-File aus und bestätigen Sie mit *Deploy*. Wenn Sie bereits eine WAR-Datei bereitgestellt haben, müssen Sie diese in der Anwendungsliste suchen und *undeploy* ausführen. Erst danach können Sie eine neue WAR-Datei bereitstellen.

3. PiSA sales Web-Client™ konfigurieren

Für die Konfiguration des PiSA sales Web Client™ melden Sie sich im Browser als Administrator an. Das PiSA sales Administrator-Servlet rufen Sie mit folgender URL auf:

`http(s)://<host:port>/<appname>/pisaadmin`

appname ist der Deployment-Name. *pisaadmin* ist der Servletname.

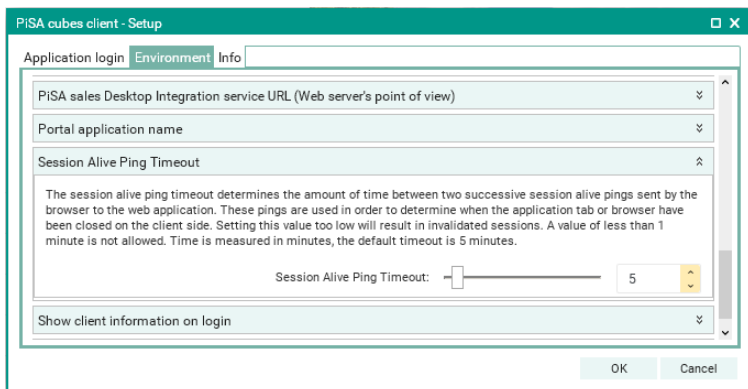


The image shows the PiSA sales Web-Client login page. It features the PiSA sales logo and a large number '7'. Below the logo, there are input fields for 'Choose Application', 'Host name', 'Port number', 'Protocol', 'User name', and 'Password'. To the right of these fields are three buttons: 'Setup...', 'User Login', and 'Load PSADIM'. At the bottom, there is a large 'Login' button with a right-pointing arrow. The footer contains the website 'www.pisasales.de', a 'Privacy' link, and an information icon.

Den Konfigurations-Dialog öffnen Sie über den Setup-Button.

Im Reiter *Application login* legen Sie die Benutzer-Login-Sets an, genauso wie für den Windows-Client. Die Sets werden im Arbeitsverzeichnis des Web-Servers gespeichert.

Im Reiter *Environment* konfigurieren Sie den Web-Client mit Hilfe verschiedener Umgebungsvariablen. Unter jedem Eintrag finden Sie die entsprechende Beschreibung und Einstellungsmöglichkeiten.



The image shows the 'PiSA cubes client - Setup' dialog box. It has three tabs: 'Application login', 'Environment', and 'Info'. The 'Application login' tab is selected. It contains several configuration options: 'PiSA sales Desktop Integration service URL (Web server's point of view)', 'Portal application name', 'Session Alive Ping Timeout' (with a description and a slider set to 5), and 'Show client information on login'. At the bottom, there are 'OK' and 'Cancel' buttons.

3.1 Umgebungsvariablen des PiSA sales Web Client™

Name	Beschreibung	Werte	Default
Automatic Download	CLI_AUT_DWN Legt fest, ob eine Datei nach Benutzeranforderung sofort an den Client übertragen wird. Falls der IE automatische Downloads nicht erlaubt, sollte diese Variable auf false gesetzt werden, damit der Web-Client einen Popup zum Download von Dateien anbietet.	true false	true
Block portal login access	PSC_POR_BLK Blockt den Zugang zum Login-Screen im Portalmodus (Anwender sieht den Login-Screen nicht). Verhindert Anmeldeversuche Dritter, wenn z.B. servergesteuerte Autologins verwendet werden.	true false	false
Block redirect	PSC_BLK_RDR Bei Verwendung Portal block können Dritte auf einen anderen URL umgeleitet werden. Der Wert der Variable ist der URL. Form wie PSC_EXI_RDR.	fixed::www.xyz.com = beliebige URL	-
Calendar windows session timeout	CAL_SSN_TIM_OUT Bestimmt wann die aktuelle Session des Kalenders als abgeschlossen gilt. Ein Session-Alive-Ping überwacht den Status der Kalender-Session. Falls der Zeitraum zwischen zwei aufeinanderfolgenden Ping-Events größer als der Timeout ist, wird die Kalender Session geschlossen.	integer	9
Client Dialog Cache	CLI_DLG_CHE Der Client-Dialog-Cache speichert Dialoge, die vom Benutzer verwendet und geschlossen wurden. Die Dialoge werden – falls möglich - beim nächsten Aufruf sofort aus dem Cache geladen. Dies erhöht die Performance.	true false	true
Client Dialog Cache Size	CLI_DLG_CHE_SIZ Legt die maximale Anzahl von Dialogen fest, die zwischengespeichert werden. Für den IE sollte –die Anzahl < 10 sein aufgrund des Speichermanagement dieses Browsers.	integer	5
Disable PiSA sales Desktop Integration	DIS_BRW_PLG Deaktiviert die PiSA sales Desktop-Integration. Funktionen, die die Integration erfordern, funktionieren dann nicht mehr.	true false	false
Exit redirect option	PSC_EXI_RDR Legt fest, welche Webseite der Benutzer nach dem Logout sieht.	Login = login screen blank = blank page fixed::www.xyz.com = beliebige URL	blank
Exit redirect timeout	PSC_EXI_RTO Steuert den Exit Redirect Timeout	xx Sekunden	10
Force Dialog Modification Bar	FRC_DLG_MOD_BAR Die Variable wird nur im Portal-Modus ausgewertet. Sie erzwingt die Anzeige eines Dialogs mit Speichern- und Abbruch-Button.	true false	false

Force TLS for PiSA sales Desktop Integration	Transport Layer Security, wenn true, dann nimmt DIM immer einen Secure socket	true false	false
Internal message count update timeout	Intervall (in Sekunden) für den Hintergrund-Task, der die Anzahl der am PiSA sales Logo des Web-Client anzuzeigenden offenen Nachrichten.		
Logging-Level of PiSA sales Desktop Integration	PLG_LOG_LVL Setzt die Logging-Stufe der PiSA sales Desktop-Integration.	TRACE DEBUG INFO WARN ERROR FATAL OFF	WARN
Message dialog title	PSC_MSG_TTL Definiert den Titel von modalen Fenstern. Der Default-Titel ist „PiSA sales client“. Mit der Variable kann z.B. der Applikations- oder der Firmenname als Titel definiert werden.	String	-
Navigation History Size	NAV_HST_SIZ Die Variable wird nur im Portal-Modus ausgewertet. Sie bestimmt die Anzahl von Dialogen, die über den "Zurück" und "Vorwärts"-Button des Browsers erreicht werden können. Sind mehr Dialoge im Stack, werden sie gelöscht. Es sollte mindestens ein Dialog im Stack erreichbar sein.	integer	5
PSC Portal Mode	PSC_POR_MOD Legt fest, ob der Web-Client im Full-Modus (false) oder im Portal-Modus (true) betrieben wird. Der Portal-Modus bietet Benutzern einen vereinfachten Zugang zum System.	true false	false
PiSA sales Desktop Integration timeout	Timeout in Sekunden bis eine Verbindung zur Desktop Integration hergestellt sein muss	integer	10
PiSA sales Desktop Integration service URL (End user's browsers point of view)	URL des PiSA sales Desktop Integration service. Hier: Der Dienst ist auf dem gleichen Web Server gehostet und hat den servlet Namen „psawsc“.	[hostname[:port]] /servlet	/psawsc
PiSA sales Desktop Integration service URL (web servers point of view)	URL des PiSA sales Desktop Integration service. Hier: Der Dienst ist auf dem gleichen Web Server gehostet und hat den servlet Namen „psawsc“.	[hostname[:port]] /servlet	/psawsc
HINWEIS: Der Service <i>psawsc</i> für die Desktop Integration sollte zuerst installiert werden, damit gleich der richtige URL konfiguriert werden kann.			
Portal application name	PSC_POR_APP Setzt den Default-Applikationsnamen für alle Benutzer global für den Portal-Modus. Der Benutzer kann beim Login keine andere Applikation auswählen. Der hier definierte Applikationsname muss in der Liste der verfügbaren Applikations-Sets (Reiter "Application login") enthalten sein.	String	-
Session Alive Ping Timeout	SSN_ALV_TIM_OUT Setzt das Session-Timeout des Web-Clients in Minuten. Dabei handelt es sich um ein Mindest-Intervall zwischen zwei aufeinander folgenden Pings vom Client (Browser) auf den Web-Server (z.B. Tomcat). Mit diesen Pings wird überwacht, ob die Anwendung noch aktiv ist oder bereits beendet wurde (siehe auch Kap. 2.3.3).	integer	5

Show Client Information on Login	SHW_CLI_NFO Ist das Feature aktiviert, werden einige Client-Informationen in der PiSA sales Meldungs-Leiste ausgegeben. Im Portal-Modus ist dieser Wert immer "false".	true false	false
URL of custom CSS definition	Wenn gesetzt, dann wird der URL an den Web Browser des Users übergeben, um zusätzliche CSS definitionen bereitzustellen.		leer

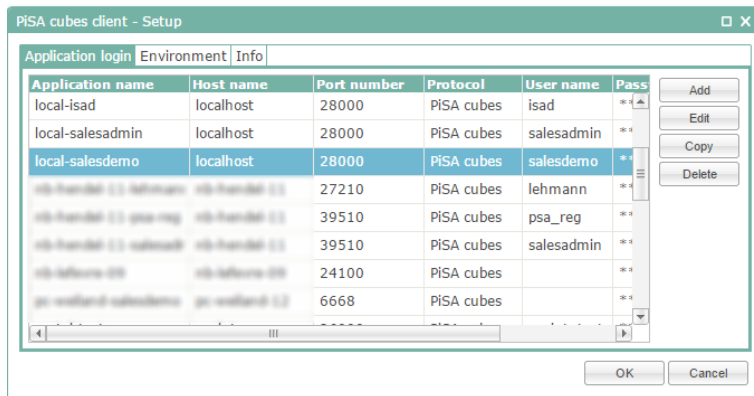
3.2 Einstellungen am PiSA sales Applikationsserver, die den Web-Client beeinflussen

Die Einstellungen finden Sie im Administrationsbereich (Administration -> Einstellungen -> Einstellungen -> Web-Client)

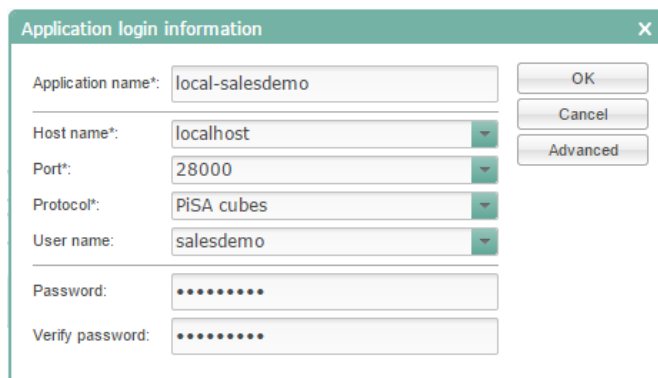
Name	Beschreibung	Werte	Default
PSC_RAP_DIS_FTS	Aktiviert oder deaktiviert die Volltext-Suche in der Toolbar. Die Volltextsuche sollte in Szenarien mit eingeschränkter Sicht/Zugriff deaktiviert werden.	y n	n
PSC_RAP_DIS_VWS	Blendet bestimmte Bereiche der Anwendung aus, wie z.B. die Hilfeleiste oder die Filterliste. Im Portal-Modus hat die Einstellung keine Wirkung. In diesem Modus sind alle ausblendbaren Bereiche automatisch ausgeblendet.	Initial{,initial} [NAV (navigator), BRW (browser), FLT (filter), FNC (function menu in dialogs), HLP (help viewer), MSG (message viewer); Example: "BRW,FLT,FNC"]	\$NONE
PSC_RAP_PRS_CAL_CPA	Definiert die Farbpalette des persönlichen Kalenders		
PSA_ACC_RAP_PRS_EXT	Steuert, ob das Login am Webclient für externe Personen erlaubt ist.	y n	y
PSA_ACC_WEB_PRS_INT	Steuert, ob das Login am Webclient für interne Personen erlaubt ist.	y n	y

4. Konfiguration der Login Sets

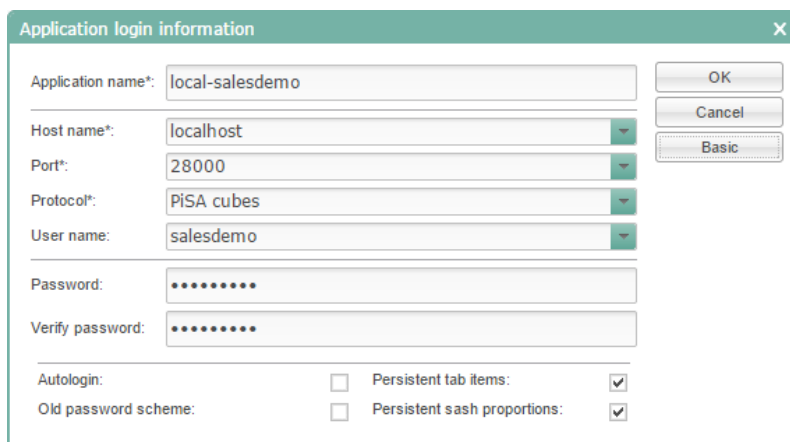
Im Administrator-Servlet legen Administratoren Login-Sets für Standard-Benutzer an.



Jedes einzelne Login-Set kann angepasst werden.



Die erweiterten Einstellungen (Advanced) ermöglichen das Konfigurieren eines Login-Sets mit erweiterten Parametern.



+ Autologin

Wenn client-getriebene Autologin-Mechanismen für dieses Login Set verwendet werden, ist das Flag zu setzen. Im Login Set müssen in dem Fall unbedingt Benutzername und Passwort hinterlegt sein.

ACHTUNG: Für Server-getriebene Autologin-Mechanismen ist das Flag nicht zu aktivieren.

+ Old password scheme

PiSA sales Server vor Version 6.2-2014 (intern 6.3) unterstützen ein anderes Passwort-Schema als neuere PiSA sales Versionen. Wenn Sie mit dem Login Set auf eine PiSA sales Version zugreifen, die älter als Version 6.2-2014 ist, dann ist das Flag unbedingt zu setzen.

+ Persistent tab items

Ist das Flag gesetzt, dann werden für dieses Login-Set sessionübergreifend die vom Benutzer zuletzt aktivierten Tabs von PiSA sales Masken gespeichert und mit dem Login geladen.

Persistent sash proportions

Ist das Flag gesetzt, dann werden für dieses Login-Set sessionübergreifend die vom Benutzer zuletzt eingestellten sash proportions von PiSA sales Masken gespeichert und mit dem Login geladen.

Sash proportions bezeichnet die vom Benutzer ggf. eingestellten Proportionsverhältnisse einer Maske (z.B. Verhältnis des Detailbereichs eines Formulars zum unteren Listenbereich).

4.1 OpenID Connect (OAuth2) für den Web-Client (erst mit 7.6 im Standard)

Der PiSA sales Web-Client unterstützt die Nutzung von Authentifizierungsdiensten zum sicheren Login. Zum Einsatz kommt OpenID Connect, "Basic flow".

Der Ablauf (Authorization Code Grant) bei PiSA sales und der Umfang der Daten sind eng am OpenID Connect Standard orientiert und für die PiSA sales-Applikationen optimiert. Jeder Anbieter eines Authentifizierungs-Services, der OpenID Connect verwendet, muss diesem Standard folgen, um die entsprechende PiSA sales-API zu nutzen.

Als Referenz zur Orientierung stellt u.a. Google eine Möglichkeit zur Verfügung, OpenID Connect zu nutzen. <https://developers.google.com/identity/protocols/oauth2/openid-connect>

4.1.1 Vereinfachter Ablauf einer OpenID Connect Authentifizierung

- + Der Client erstellt eine Authentifizierungsanforderung mit den gewünschten Anforderungsparametern (engl. Request Token).**
- + Der Client sendet die Anforderung an den Autorisierungsserver (OIDC Provider mit Authentifizierungsseite).**
- + Der Autorisierungsserver authentifiziert den Endbenutzer.**

Nur wenn das erfolgreich ist, wird das Anmelden an PiSA sales fortgesetzt. Scheitert die OpenID-Connect-Authentifizierung, so erfolgt die Meldung an den Anwender. Der PiSA sales-Server wird im Fehlerfall überhaupt nicht kontaktiert.

- + Der Autorisierungsserver sendet dem Endbenutzer (Client) eine Antwort mit Authentifizierungscode zurück.
- + Der Client sendet den Code an den Token-Endpoint, um in der Antwort ein Zugriffstoken und ein ID-Token (Benutzerinformationen) zu erhalten.
- + Der Client überprüft die Token und hat Zugriff auf die Subject-ID des Endbenutzers.
- + Bei erfolgreicher Rückmeldung werden die gelieferten Informationen an den PiSA sales Server weitergeleitet und er kann die Anmeldung erlauben oder verweigern.

4.1.2 Voraussetzungen

Umgebung und Versionen

- + Web-Client ab Version 7.5.0.20200923054500
- + Der Browser muss Popups für den Web-Client erlauben.
- + PiSA sales App-Version ab 1.4.100
- + Server ab Version 7.6.
- + Ein entsprechender Authentifizierungsdienst ist verfügbar und eingerichtet.

Benötigt werden weiterhin

- + URI des OpenID-Discovery-Dokuments
(s.a. https://openid.net/specs/openid-connect-discovery-1_0.html) oder
- + URI des Authentifizierungsservers
- + URI des Token-Endpunktes
sowie
- + Client-ID (Kennzeichen)
- + Client Secret (Schlüssel)
und

Redirect URI

als geeigneter Endpunkt für die Rückmeldung des Authentifizierungsdienstes.

Wird von Web-Client bzw. Touch-Backend zur Verfügung gestellt, es muss passend zur Umgebung hier angegeben werden.

Client ID und Client Secret

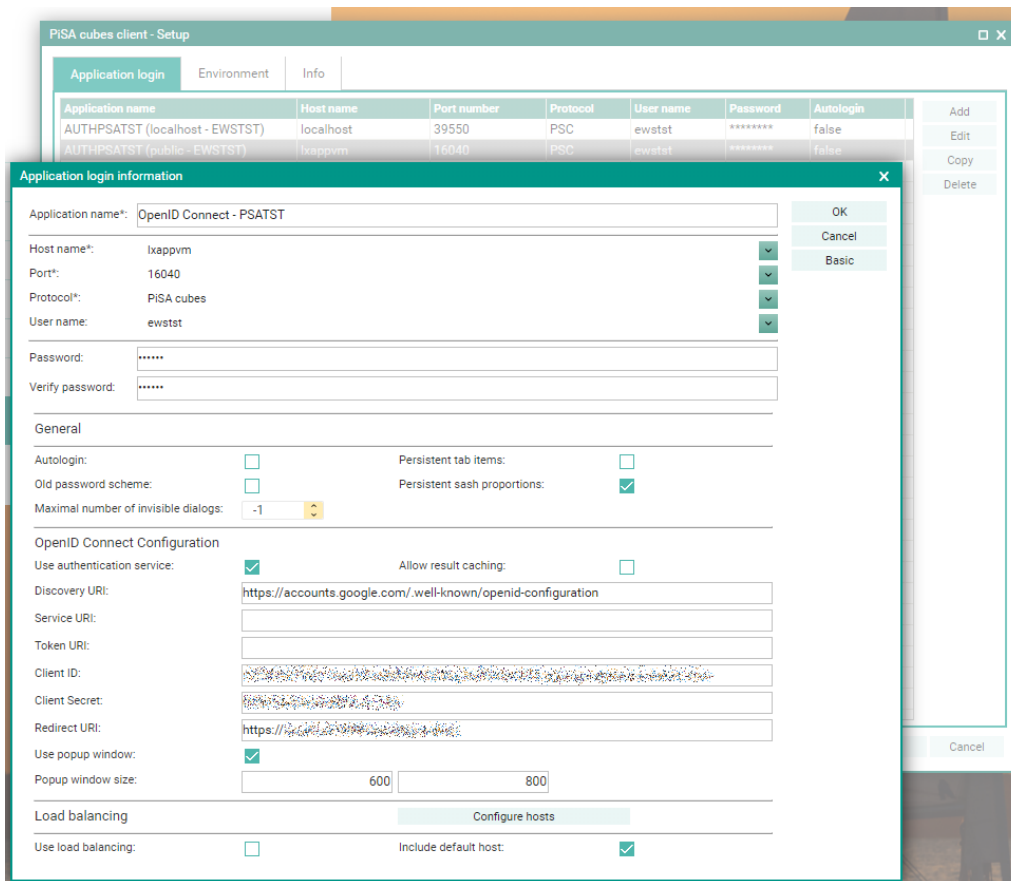
Mit Kennzeichen bzw. Schlüssel meldet sich die jeweilige Applikation beim OIDC-Provider und stellt die Zuordnung zu einer Domäne mit validen Benutzerkonten her. Der jeweilige OIDC Provider bietet eine Registrierungsseite an, wo die Client ID erstellt und der Applikation/App zugewiesen wird. Gleichzeitig wird auf dieser Seite in der Regel auch der Client Secret erstellt.

Der Client Secret wird nicht in der nativen App gespeichert, sondern mit dieser Konfiguration an der jeweiligen App ausgeliefert.

OpenID Connect (OAuth2) Einrichtung am Web-Client

Die Konfiguration des Authentifizierungsdienstes selbst wird nur dort mit den dort verfügbaren Mitteln vorgenommen. Die benötigten Informationen werden dann im PiSA sales Web-Client hinterlegt.

Die Login-Konfiguration erfolgt in der Administrations-Sicht (Admin-Konsole) des Web-Clients:



PiSA sales client - Setup

Application name	Host name	Port number	Protocol	User name	Password	Autologin
AUTHPSATST (localhost - EWSTST)	localhost	39550	PSC	ewstst	*****	false
AUTHPSATST (public - EWSTST)	ixappvm	16040	PSC	ewstst	*****	false

Application login information

Application name*: OpenID Connect - PSATST

Host name*: ixappvm

Port*: 16040

Protocol*: PiSA cubes

User name: ewstst

Password: *****

Verify password: *****

General

Autologin: ☐ Persistent tab items: ☐

Old password scheme: ☐ Persistent sash proportions: ☒

Maximal number of invisible dialogs: -1

OpenID Connect Configuration

Use authentication service: ☒ Allow result caching: ☐

Discovery URI: <https://accounts.google.com/.well-known/openid-configuration>

Service URI:

Token URI:

Client ID:

Client Secret:

Redirect URI: <https://accounts.google.com/...>

Use popup window: ☒

Popup window size: 600 800

Load balancing

Use load balancing: ☐ Include default host: ☒

4.1.3 Nutzung des Discovery-Dokuments

Die PiSA sales Applikationen erwarten den URI des OpenID Discovery-Dokuments, das der jeweilige Dienstanbieter bereitstellt

(siehe https://openid.net/specs/openid-connect-discovery-1_0.html, Punkt 4.

Hinweis: Eine vorgeschaltete zusätzliche Abfrage über WebFinger zur Ermittlung des Dienstanbieters selbst wird nicht unterstützt.

Es werden die URIs für die zwei Dienste des OIDC Providers benötigt, die als Parameter einzutragen sind.

Von der OpenID Connect Spezifikation empfohlene Konfiguration bevorzugen

Die von der OpenID Connect Spezifikation empfohlene Konfiguration ist immer vorzuziehen. Es wird ein global verfügbarer Discovery URI eintragen, wo die Zielressource die zwei weiteren URIs für den Authentifizierungscode und für den Token-Zugriff definiert.

Dieser URI ist z.B. für den OpenID Connect Dienst von Microsoft:

<https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration>

(Angaben ohne Gewähr).

Der Discovery URI wird im entsprechenden Feld eingetragen, und die zwei weiteren Felder werden automatisch gefüllt, je nachdem was in der Ressource des Discovery URI definiert wurde. Der Discovery URI wird dann in regelmäßigen Stunden-Abständen abgefragt.

Alternative ohne Discovery URI

Wird keine „Discovery URI“ eingetragen, sind die zwei benötigten URIs in die Felder für „Service URI“ und „Token URI“ als Link einzutragen und die Konfiguration zu speichern.

- + Service URI ist der URI für den Authentifizierungscode
- + Token URI ist der URI für den Zugriffstoken bzw. weitere Autorisierung

Hinweis: Der Web-Client kann nur eine Plausibilitätsprüfung vornehmen, die Angaben aber nicht vollständig validieren.

Ob ein Popup oder ein regulärer Browser-Tab geöffnet werden soll, richtet sich nach dem Authentifizierungsdienst, ebenso die eingestellte Größe des Popup-Fensters.

Redirect URI

Der Authentifizierungsdienst wird den Browser des Anwenders veranlassen, ein HTTP "GET" mit diesem Ziel aufzurufen. Der Web-Client stellt dafür einen geeigneten Endpunkt zur Verfügung (z.B.: <https://crm.company.com/pisasales/authrdr>).

Ist der Web-Client jedoch in einer lokalen Umgebung mit privater TCP-Domain installiert, dann ist ggf. eine geeignete Umleitung auf Netzwerkebene einzurichten, falls der Authentifizierungsdienst nur öffentliche Adressen akzeptiert (z.B. Google).

Behandlung von OpenID Connect im Server

Die Server-Versionen (DEV)/7.6 und 07.05-20190904 (ab 10.07.2020) unterstützen die Information vom Client, dass dieser OpenID Connect Authentifizierung beherrscht

(`de.pisa.psc.srv.gui.CLI_ENV.OID` bzw. `de.pisa.psc.srv.gui.CLI_ENV.canOpenIDC(PscGui)`).

Wenn ein Client dieses Flag beim Start der Session gesetzt hat, dann wird im Passwort-Handshake (`de.pisa.psc.srv.dsi.PscAcc.PscAcc(PscSsn, String, String)`) die Aktion "PSC_INI_PWD" erweitert zum Client geschickt.

Hat der Client keine OpenID Connect Authentifizierungsinformationen, dann wird wie bisher mit Passwort-Vergleich (Vergleich der Hash-Operationen) fortgefahren.

Hat der Client jedoch OpenID Connect Authentifizierungsinformationen gesendet, dann wird die neue Methode `de.pisa.psc.srv.gui.PscGui.evloIdNfo(int, String, String, String, boolean)` aufgerufen, deren Aufgabe es ist, diese Informationen auszuwerten und die Session ggf. erfolgreich einzuloggen.

Der (Web-) Client wird `CLI_ENV.AUT` immer auf "N" setzen, wenn mit OpenID Connect Authentifizierungsinformationen gearbeitet wird. Es ist die Aufgabe des Servers (`de.pisa.psc.srv.gui.PscGui.evloIdNfo(int, String, String, String, boolean)`), `CLI_ENV.AUT` auf "Y" zu setzen, wenn die Auswertung der OpenID Connect Authentifizierungsinformationen zum erfolgreichen Login der Session geführt hat.

4.1.4 Umfang der OpenID Connect Authentifizierungsinformationen

Der Client sendet einen reduzierten ID Token. Siehe dazu https://openid.net/specs/openid-connect-basic-1_0.html, - Abschnitt 2.2.

- **sub:** (Subject Identifier).
Erforderlich! Eindeutige Kennung des Ausstellers (OIDC Provider) für den Endbenutzer, die vom Client verwendet werden soll.
- **aud:** (Audience)
Erforderlich! Zielgruppe(n), für die dieser ID-Token bestimmt ist. Er muss die OAuth2 Client ID für PiSA sales bzw. für die Touch-Devices enthalten.
- **uri:** (URI of authentication service)
Zusätzliche Information, damit sichergestellt ist, dass nur zugelassene Authentifizierungsdienste akzeptiert werden.

Da die eigentliche Authentifizierung schon erfolgt und der ID Token somit schon ausgewertet ist, wird in **aud** stets nur die "Client ID" als einfacher String gesendet.

Beispiel aus der PiSA sales Test-Umgebung bei Google:

```
{"sub": "103534874923994555439", "aud": "123362673637-kssc2vo8d99v9on5hq71o066cen207j.apps.googleusercontent.com"}
```

Innerhalb eines Authentifizierungsdienstes ist der Subject Identifier **sub** stets eindeutig. Da aber nicht auszuschließen ist, dass mehr als nur ein Authentifizierungsdienst genutzt wird, ergibt sich die Eindeutigkeit für PiSA sales Accounts nur in der Kombination aus **sub** und **aud**.

4.1.5 OpenID-Konfiguration

Menü Administration/Kontakte/OpenID/Konfiguration

In der Liste werden zwei Informationen verwaltet.

- Discovery-**URI**, also der global verfügbare URI des Authentifizierungsservers
 - z.B. für Google: <https://accounts.google.com/.well-known/openid-configuration>
- die Client ID **AUD** (Applikationen-ID), die beim Authentifizierungsserver angemeldet sind
 - bei PiSA sales der Web-Client und die Clients auf den Geräten, wobei sich die Applikationen für iPad, iPhone und Android phone auf den Geräten unterscheiden und zurzeit noch einzeln angemeldet sein müssen (da die Authentifizierung noch direkt an das Gerät zurück geht und nicht an den Server)

Zur Info: Perspektivisch wird die Authentifizierung für die Geräte nicht auf das Gerät, sondern auch an den Server gesendet (wie für den Web-Client).

4.1.6 OpenID-Benutzer

Menü Administration/Kontakte/OpenID/Benutzer

In der Liste „Open-ID-Benutzer-Zuordnung“ werden PiSA-Benutzer und OpenID-Benutzer gemappt. Der Authentifizierungsdienst übergibt per Token beide Informationen an das System, und es wird geprüft, ob PiSA-Benutzer und OpenID-Benutzer übereinstimmen. Die Anmeldung an der Domäne über die OpenID-Authentifizierung wiegt höher als die Anmeldung mit Passwort.

Hinweis: Ist ein PiSA-Benutzer in der Liste eingetragen und die Authentifizierung erfolgreich, dann wird der Zugang freigegeben, unabhängig davon, ob das PSA-Passwort eingegeben wurde oder nicht (zu vergleichen mit dem Auto-Login am Web-Client).

Zur Bearbeitung/Steuerung der Zuordnungen sind Admin- bzw. Kontaktadmin-Rechte erforderlich.

Unterstützung durch Variablen

PSA_SFR_OID_SUP

Server-Feature: OpenID Unterstützung in PiSA sales = n/y. Bei „y“ erfolgt die Prüfung, ob für den PiSA-Benutzer ein OpenID-Benutzer zugeordnet ist. Wird keine Zuordnung gefunden, kann die zweite Variable für den User (SUB) automatisch eine Zuordnung erzeugen.

PSA_OID_ADD_USR_SUB

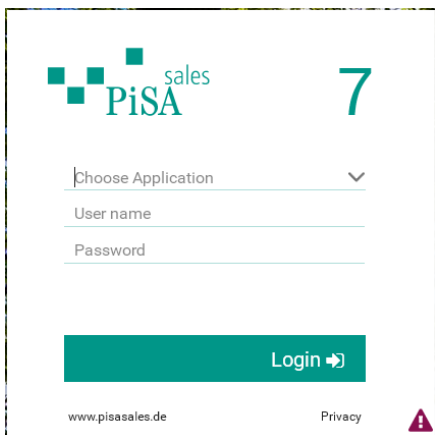
OpenID: ordnet dem Benutzer automatisch die OpenID-Kennung zu, aber nur, wenn es noch keine Zuordnung für diesen Benutzer gibt. Im Ergebnis wird dann künftig immer nur auf diese OpenID-Zuordnung authentifiziert.

5. Benutzer-Login

Standard-Benutzer melden sich an, indem Sie ein (vom Administrator angelegtes) Login-Set anhand des Applikationsnamens auswählen. Das PiSA sales-Servlet rufen Sie mit folgender URL auf:

`http(s)://<host:port>/<appname>/pisasales`

appname ist der Deployment-Name. *pisales* ist der Servletname.



5.1 URL-Parameter

Das Login kann bei Bedarf über zusätzliche URL-Parameter vereinfacht/automatisiert werden.

Name	Beschreibung	Beispiel
login	Vereinfachtes Login mit vordefiniertem Applikations- und Benutzernamen. Der Benutzer muss nur sein Passwort eingeben. Die Applikation muss existieren. Parameterstring ist: <username>@<application>	<code>http://localhost/pisa?login=salesdemo@psatst</code>
	Autologin mit vordefiniertem Applikationsnamen, Benutzernamen und Passwort. Es muss ein vollständig definiertes Login-Set mit Benutzername und Passwort existieren. Im Set muss das Autologin-Flag gesetzt sein (wird über den Advanced-Button im Login-Set sichtbar). Parameterstring ist: <application>	<code>http://localhost/pisa?login=psatst-salesdemo</code>
	Serverunterstütztes Autologin. Die URL enthält einen String, der vom Server ausgewertet und verifiziert wird. Eine solche URL kann z.B. per E-Mail an den Benutzer versendet werden, z.B. um Fragebögen über den Web-Client zu erfassen. Parameterstring ist: autowlgi<xyz>@<application>	<code>http://localhost/pisa?login=autowlgiXYZ@psatst</code>
sww	Aktiviert das Watch-Window. Das Watch-Window zeigt Informationen für Entwickler/Customizer in der Meldungsleiste an. Zugelassene Werte sind: {true,false}	<code>http://localhost/pisa?sww=true</code>

5.2 Installation der PiSA sales Desktop-Integration

Die für die Kopplung zwingend benötigte Desktop-Integration wird weitgehend automatisiert als *Desktop Integration Manager* (DIM) installiert. Es sind keine Administratorrechte erforderlich.

5.2.1 Installationsvoraussetzungen

Für das Installieren und Ausführen sind folgende Software und Freigaben erforderlich:

- + .NET Framework 4.5 und größer
- + VSTO-Runtime (nur für Office 2010) mind. Version 4.0

Freigaben:

- + Download + Installation von MSI-Dateien muss erlaubt sein (Virenschanner?)
- + Client-PC muss PSAWSC-Server erreichen können (Firewall?)

Bei Verwendung eines Proxy-Servers:

- + Proxy mit HTTPS-Websocket Unterstützung

5.2.2 Desktop-Integration installieren:

Beim ersten Login im Web-Client wird automatisch vom Web-Client ein *.msi-File zum Download angeboten. Sind die Installationsvoraussetzungen erfüllt, muss es ausgeführt werden, um die Desktop-Integration zu installieren.

Im Login-Dialog der PiSA sales Startseite wird ein orangefarbenes Dreieck dargestellt, falls es Probleme mit der Office-Kopplung gibt. Die Desktop-Installation prüft dafür, welche Office-Programme installiert sind, ob die PiSA sales-Addins korrekt installiert sind und ob die aktuelle VSTO Version 4.0 (Office-Komponente von MS) verfügbar ist. Insgesamt werden damit folgende Zustände visualisiert:

- Desktop-Integration arbeitet korrekt -> Grünes „i“
- Probleme mit der Office-Kopplung -> Oranges Dreieck
- Mindestens ein fehlendes Addin -> Grünes Dreieck
- Desktop-Integration nicht verfügbar oder nicht aktuell -> Rotes Dreieck

Nutzen Sie die Informationen im Kontrollfenster, dass Sie mit Klick auf das entsprechende Symbol öffnen.

Der Desktop Integration Manager (psadim.msi) ist „per user“ zunächst selbst zu installieren und läuft dann automatisch als Hintergrundprozess (Tray).

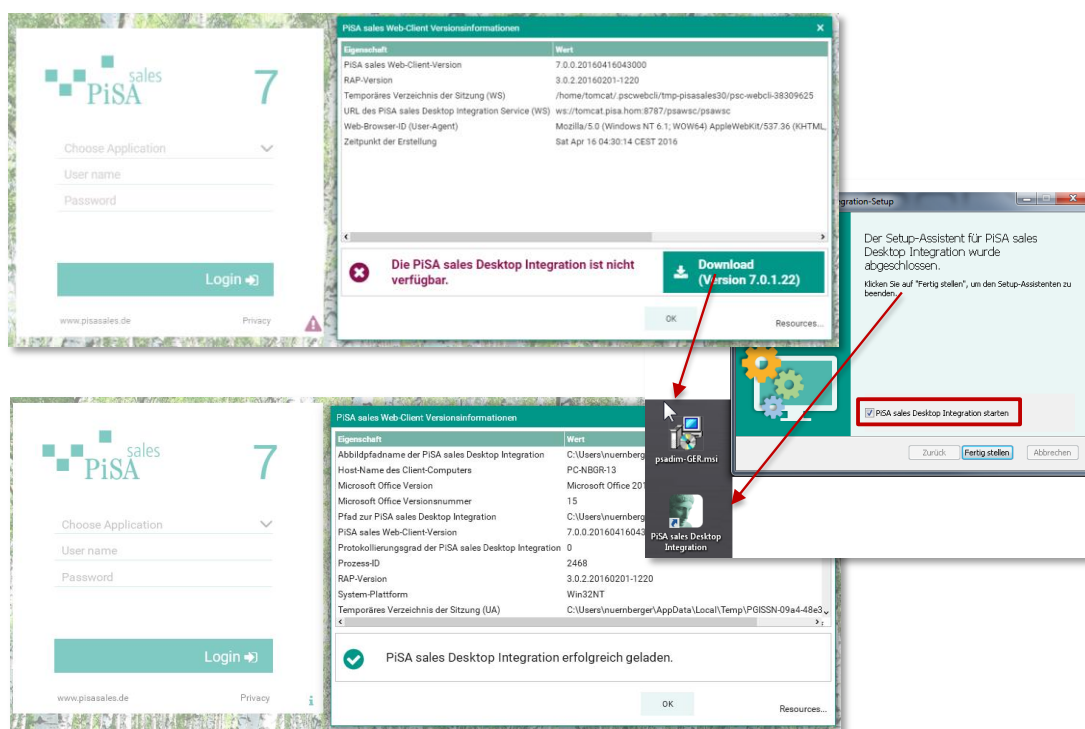
Ist der Desktop Integration Manager noch nicht installiert bzw. nicht mehr aktuell, dann erscheint mit Aufruf der Web-Client-URL im Internetbrowser ein Warndreieck rechts unten im PiSA sales Login-Dialog, die auf die eventuell deaktivierte/nicht aktuelle Desktop-Integration hinweist.

ACHTUNG: Beim ersten Aufruf müssen Sie im Internetbrowser die Abfrage, ob die externe Applikation bzw. der externe URL ausgeführt werden darf, mit JA bestätigen. Am besten setzen Sie die entsprechende Einstellung auf „*immer diese Aktion ausführen*“, um nicht jedes Mal neu bestätigen zu müssen.

Folgende Schritte sind bei Erfordernis zu unternehmen:

Desktop Integration noch nicht installiert:

1. Warndreieck anklicken und „*Download*“ ausführen (*psadim-LNG.msi* beliebig lokal ablegen). Alternativ finden Sie den Link zur Installationsdatei in der Liste „Ressourcen“ (zusätzlicher Button).
2. Groupware-Programme und Office-Programme beenden.
3. *psadim-LNG.msi* ausführen und installieren.
4. Internetbrowser öffnen und PiSA sales-URL aufrufen bzw. Seite neu laden (Aktualisieren).
5. Ist der Desktop Integration Manager erfolgreich gestartet, dann ist das Warndreieck im Login-Dialog gegen ein Ausrufezeichen ersetzt, und die Desktop Integration ist auch als Prozess im Tray zu sehen.



Desktop Integration nicht aktuell:

- Ist die Desktop Integration nicht aktuell, erscheint ebenfalls ein Warndreieck im Login-Dialog. Dann ist der Desktop Integration Manager erneut herunterzuladen und zu installieren (siehe oben).

PopUp-Blocker deaktivieren!

Um alle Features nutzen zu können (z.B. Persönlicher Kalender) muss das Blockieren von Popups im verwendeten Browser einmalig für den Web Client deaktiviert werden. Der entsprechende Hinweis dazu wird dem Benutzer gleich beim ersten Aufruf des Kalenders angeboten, wenn Popups gesperrt sind. Für Details, wie Popups in Ihrem verwendeten Browser deaktiviert werden, informieren Sie sich bitte in der Hilfe/Dokumentation des jeweiligen Browsers.

HINWEIS: Insbesondere bei Verwendung des Google-Chrome-Browsers gibt Chrome nur einen kurzen Hinweis auf ein blockiertes PopUp und danach erfolgt keine weitere Information. Das Entsperren von PopUps unter Chrome geschieht dann nur über ein Icon in der URL-Bar. Das ist bei Chrome tatsächlich die einzig angebotene Möglichkeit, PopUp-Blocker zu verwalten.

Achtung bei paralleler Win-Client-Installation

Wird neben dem Web-Client auch der Win-Client genutzt, dann muss mit Aktualisierung der DIM der Win-Client neu installiert werden!

5.2.3 PiSA sales Desktopintegration (DIM) im Browser zulassen

Beim PiSA sales Login im Browser Google Chrome oder Edge Chrome werden Sie immer gefragt, ob die PiSA sales Desktop Integration geöffnet werden soll. Will man diese Abfrage unterbinden bzw. immer automatisch zulassen, dann können folgende Maßnahmen helfen.

Die Entwickler der Browser ermöglichen das ohne administrativen Eingriff nicht mehr. Der Browser Chrome sieht in den aktuellen Versionen ab 77 die Möglichkeit nicht mehr vor, durch den Anwender ein sog. "Merken"-Häkchen zu setzen. Auf dieses Browser-Feature hat die PiSA sales Entwicklung keinen Einfluss.

Sie können jedoch mit geeigneten Registry-Einträgen dafür sorgen, dass diese "Merken"-Option wiedererscheint.

Google Chrome

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
Value Name: ExternalProtocolDialogShowAlwaysOpenCheckbox
Value Type: REG_DWORD
Value Content: 0x00000001 (1)

Microsoft Edge Chromium

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
Value Name: ExternalProtocolDialogShowAlwaysOpenCheckbox
Value Type: REG_DWORD
Value Content: 0x00000001 (1)

Diese Werte sollten also vorzugsweise über eine Policy gesetzt werden.

Gar keine Rückfrage oder automatisches Zulassen erreichen Sie durch folgendes Vorgehen.

Nur Google Chrome Enterprise

Hier gibt es die Möglichkeit, die fraglichen Protokolle in eine Whitelist aufzunehmen (verifiziert!):
(<https://t-e.cc/google-chrome-no-longer-displays-always-open-these-types-of-links-in-the-associated-app-checkbox-fix/>).

Dazu müssen unter [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\URLWhitelist] die Werte angelegt werden, auch das vorzugsweise per Policy.

- "1"="psadims://*"
- "2"="psadim://*"

In diesem Fall erfolgt gar keine Rückfrage mehr, sondern der Browser wird die Protokolle akzeptieren und die Verbindung zur Desktop-Integration veranlassen.

Nur Google Chrome

Es ist ggf. auch möglich, einen Eintrag im lokalen Properties-File des Browsers vorzunehmen, der dafür sorgt, dass die PiSA sales Desktop Integration automatisch zugelassen wird
(<https://support.google.com/chrome/thread/14193532?hl=en>).

Die Konfigurationsdatei findet man unter Windows in dem Pfad
„C:\Users\<Username>\AppData\Local\Google\Chrome\User Data\Default\Preferences“.

Der hinzuzufügende Eintrag ist folgender:

- "protocol_handler":{"excluded_schemes":{"psadim":false,"psadims":false,"sfb":false}}

Weiterführende Links für **Edge Chromium**:

<https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies>

<https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#externalprotocoldialogshowalwaysopencheckbox>

6. Portable Web-Client-Anwendung

Der portable Web-Client wird hauptsächlich als Workaround bereitgestellt, um den Web-Client alternativ nutzen zu können, wenn es mit bestimmten Browsern schwerwiegende Probleme gibt.

Auf Anforderung wird die portable Anwendung durch die PiSA sales Entwicklung als ZIP-File bereitgestellt, das unter anderem eine EXE-Datei mit dem Namen "psawebcli.exe" und alle erforderlichen Bibliotheken (DLLs) enthält. Dabei handelt es sich um eine stark reduzierte Light-Version des Chrome-Browsers (derzeit in der Version 66), der als festen URL die Zieladresse der Web-Client-Umgebung des Kunden aufruft.

Das heißt, dass für jeden Kunden, der die portable Anwendung nutzen möchte, ein eigenes solches ZIP-File erstellt wird, wo der Aufruf der Web-Client-Umgebung des Kunden als fester URL integriert ist. Der Kunde kann dieses ZIP-File an seine Anwender verteilen. Es wird ganz ohne Installation einfach entpackt und im Zielordner dann die "psawebcli.exe" gestartet. Daraufhin wird automatisch die Log-In-Seite des Web-Clients der PiSA sales-Applikation des Kunden geöffnet.

Die Vorteile der portablen Anwendung sind:

- + sehr schnell
- + maximale Bildschirmnutzung, weil keine Adressleiste, kein Lesezeichen usw. vorhanden sind
- + sie ist unabhängig von Browser-Vorgaben durch Konzerndirektive u.ä.

Zu berücksichtigende Einschränkungen:

- + exakt nur ein URL (eine Web-App) erreichbar
- + keine Rechtschreibprüfung verfügbar
- + nicht für administrative Zwecke nutzbar (kein Admin-URL)
- + keine "Vorwärts" und "Rückwärts"-Navigation im Browser