iPortalis Limited

Data Security Framework and Policies for iPortalis Control Portal (iCP)

Updated: March 2017

CONTENTS

Introduction

This security framework document supports the iPortalis proposal to implement functionality, processes and connections for the iPortalis Control Portal (iCP) to allow Client Administrators to manage Microsoft O365 licence provisioning and integrate iCP into the Client O365 tenant.

The security does not just apply to the iCP software, but also to our operational processes, tools and personnel.

Goal

The goal of this document is to demonstrate to Client that iPortalis Limited is a technically and operationally security compliant service provider.

The document shows:

- Operational policies
- Communication and Operations network diagrams
- Client O365 tenant threat analysis
- AD property entity details
- Data awareness
    - Storage
    - Security
    - Integrity
    - Transit

iPortalis Security Framework

The following section will demonstrate iPortalis operational security compliance.

Data Protection Act

The Information Commissioners Office has registered iPortalis under the data protection act with registration reference **ZA208153**.

Policy

iPortalis has the following security policies:

- Anti-piracy policy
- Network system monitoring policy
- Remote access and mobile computing policy
- Virus protection policy
- Leaving policy
- Access control policy

iPortalis also has the following operations policies in place:

- Change Management policy
- Release Management Policy
- Continuity Policy

Compliance

The following will demonstrate iPortalis compliance in relation to specific operational processes.

Access Control

Sub Section	Requirement
Network Access Control	The structure of the network controls equipment identification.
Network Access Control	Authentication of remote diagnostic ports is controlled.
Network Access Control	Network segregation controls are included in the Access Control Policy and are as defined in the Network Structure Diagram.
Operating Systems Access Control	IP address connections are either static IP's assigned according to defined rules or are dynamically issued by the system.
Operating Systems Access Control	User identification and authentication requirements are defined and allocated by the Systems Department and are addressed in the Access Control Policy.
Operating Systems Access Control	Access to system utilities is restricted to the Systems and/or Technical Support teams with the necessary authorisation.
Operating Systems Access Control	Requirements for session time-outs are defined in the Access Control Policy and provide for limited time-outs for in-house use with more stringent and enforced time-outs for any external connections.
Application Access Control	Information access restrictions are imposed.
Application Access Control	Sensitive systems, applications and data are isolated using a combination of physical and electronic controls.

Business Continuity

Sub Section	Requirement
Information security aspects of business continuity	A Business Continuity Plan (Disaster Recovery) is documented. The Business Continuity Plan includes procedures for timely restoration of business following interruption or failure of critical business processes.
Information security aspects of business continuity	The Business Continuity Plan includes a single framework ensuring consistency and the establishment of priorities.

Communications and Operations

Sub Section	Requirement

Operational Procedures and Responsibilities	Any source, test and development code is clearly identified and protected from the production environment.
Operational Procedures and Responsibilities	Hardware firewall, virus and spyware protection are run continuously.
Operational Procedures and Responsibilities	The logs are checked automatically against pre-defined rules and checked on a regular basis.
Network Security Management	Security of network services are identified in the SLA and/or contract established and agreed with the customer, contractor, third-party provider.
Electronic Commerce	Systems relating to electronic commerce transaction are in place and these have been developed to achieve security and management of risk.
Electronic Commerce	On-line transactions are carried out using industry standard security and encryption using, in most cases, recognised third-party providers. Financially-sensitive information is not accessible to employees and the transaction record is deleted after the support period.
Monitoring	Log information is held as a system record and protected as defined in our Security Manual.
Monitoring	Clock synchronisation is carried out as a component of the operating system utilities, including automatic verification with an on-line source of time data and automatic daylight saving time changes.

EQUIPMENT SECURITY

Sub Section	**Requirement**
Responsibility for Assets	An inventory of critical assets is maintained in the DHL
Responsibility for Assets	Ownership of assets is maintained in the DHL
Equipment Security	Equipment siting and protection – appropriate security and preventative measures are in place
Equipment Security	UPS's are connected to the office servers with a minimum run time of 20 minutes.
Equipment Security	Precautions are taken to ensure the security of cabling within the premises.
Equipment Security	Equipment maintenance is carried out by authorized personnel
Equipment Security	Support contracts are in place with key equipment suppliers.
Equipment Security	A specialised company is used in disposal of assets and records of disposals are kept.

THIRD PARTIES

Sub Section	Requirement
External Parties	Third party access risks are addressed as part of routine maintenance of the DR plans
External Parties	Non-disclosure agreements are in place with third party contractors as part of contract or included in SLA
External Parties	Protection of assets are defined within the third party contract or SLA
External Parties	Risk associated with third parties is defined in DR plans

HUMAN RESOURCES

Sub Section	Requirement
Prior to employment	Employee screening and policy – CRB checks carried out prior to employment or during first 2 weeks of probationary period.
Prior to employment	Terms and conditions of employment from part of the employees contract. Signed copy retained in HR file.
During employment	Staff are inducted into the organization and given access to the ISMS Manual and policies.
During employment	An induction sheet is signed and retained in the HR file.
During employment	Information security awareness, education and training.
Termination of employment	A leaving policy is in place and the process is followed.
Termination of employment	All company assets are recovered as part of the leaving process.
Termination of employment	The leaving checklist must include check to identify IT Team of a leaver and ensure all system and physical access is removed.
Physical and environmental security	Physical security perimeters are reviewed.
Physical and environmental security	Physical entry controls and reviewed.
Physical and environmental security	The HQs server rooms are accessible only by authorized personnel, and a list is held of those authorized.
Physical and environmental security	Public access areas are controlled and limited. All visitors are accompanied at all times.

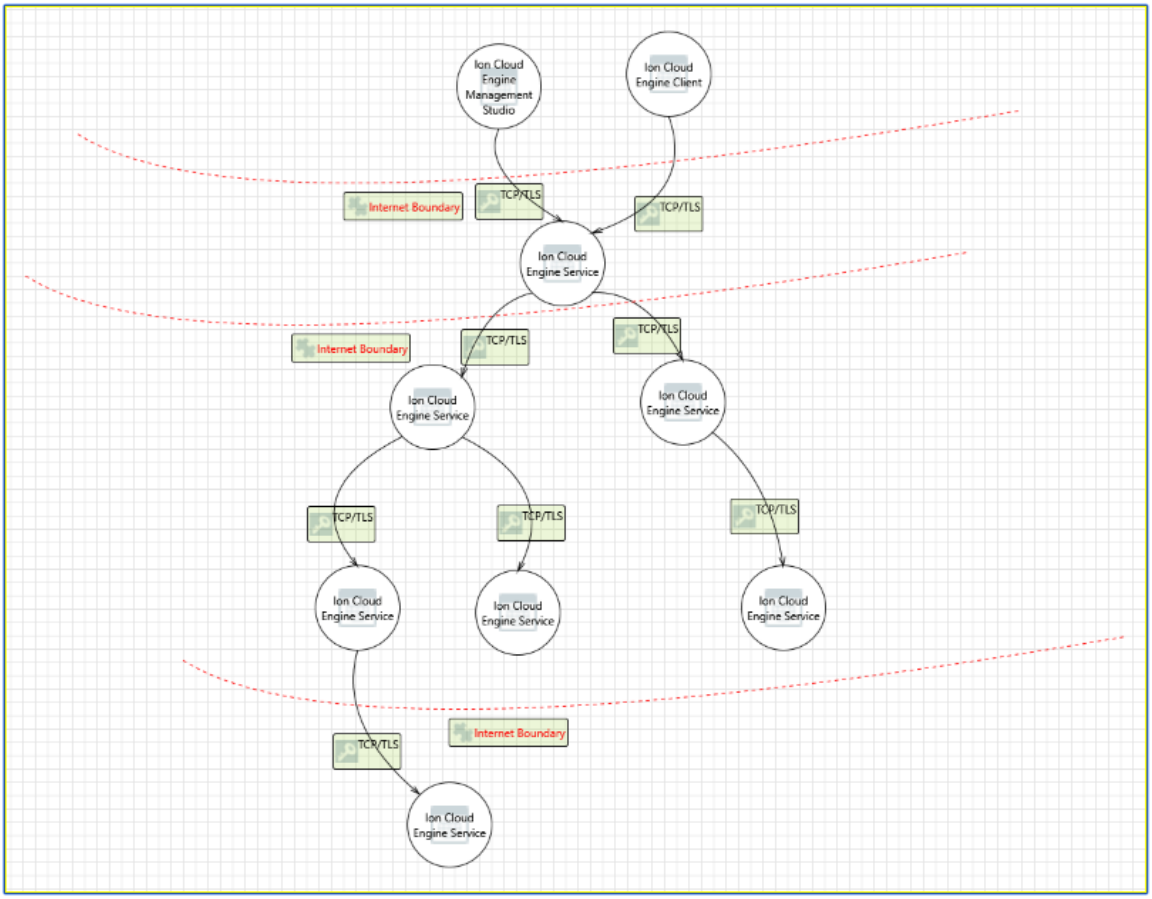
SYSTEMS

Sub Section	Requirement
Security Requirements of Information Systems	Security requirements for new or enhanced systems are determined and specified by the Organisation and documented as part of the system specification.
Correct Processing in Applications	Data input validation requirements are limited to the data field parameters incorporated into the designed system. Data is validated, approved and/or tested prior to final entry into the system and release to a live environment.
Correct Processing in Applications	Internal processing controls are contained within the application.
Correct Processing in Applications	Any data validation checks required are automatic and carried out as part of system operations. Additional load and/or stress testing and related output validation is carried out where considered necessary.
Security of System Files	Licenses for the use of software on the Organisation's systems are valid and in date. A Software Licence and Usage Register is in place and reviewed regularly.
Security of System Files	All appropriate protection is given to test data. The use of specific file names prohibits the test data being available to live applications.
Security of System Files	The Organisation develops generic and client-specific code. An industry standard source code protection utility is used to control this area and access is limited.
Security in Development and Support Processes	The Systems Team monitors information when new vulnerabilities are announced to be able to correctly assess the vulnerability of their exposed systems and to take preventive/corrective action. Changes to systems are recorded.
Security in Development and Support Processes	Software development partnerships may be in place. Where this occurs, a Service Level Agreement is established and signed by both parties defining the scope, responsibilities and issues including copyright and intellectual property rights. A copy is signed and retained by both parties.
Technical Vulnerability Management	Technical vulnerabilities identified as a result of the implementation of the ISMS are reviewed and addressed.

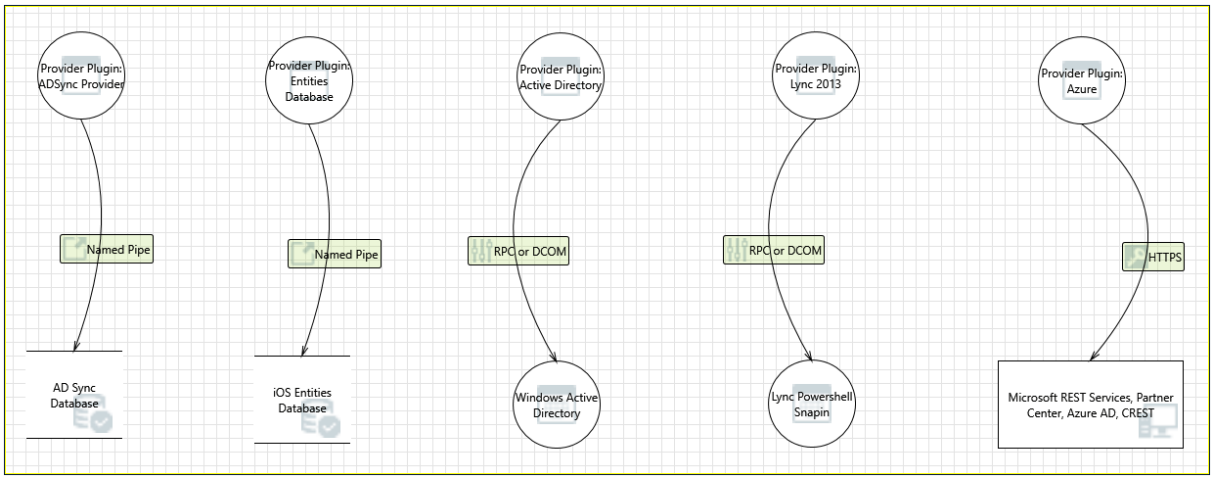
Client o365 Tenant Integration Requirement

Communications and Operations

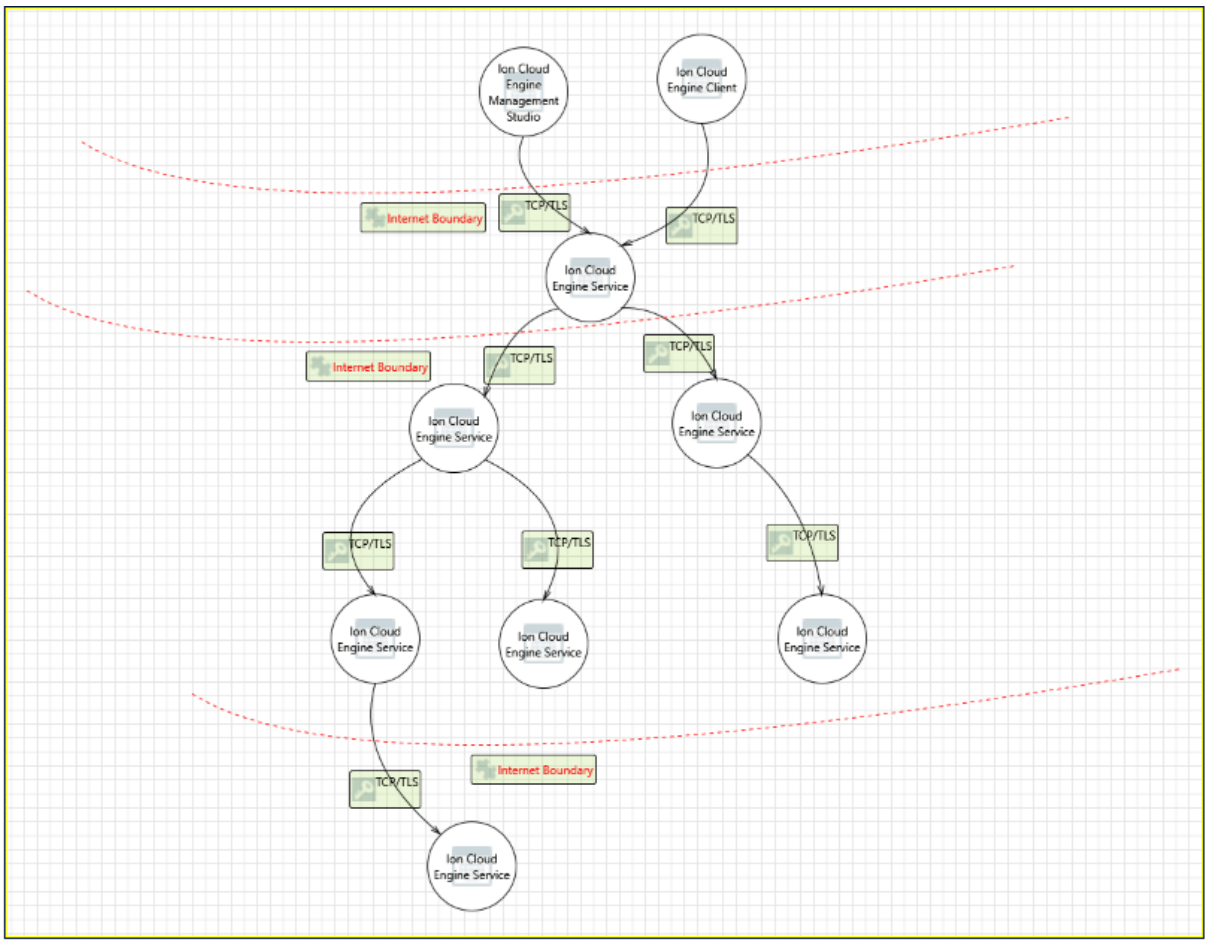
iCP Engine Network Diagram



iCP Engine Provider Plug Ins Network Diagram



ICP ENGINE SERVICE NETWORK DIAGRAM



O365 Threat Modelling Report

Threat Model Name: iCP Engine integration with Office 365 REST APIs

Description: This threat model provides an overview of identified threats and the mitigation for those threats in iPortalis interaction with Microsoft APIs related to Office 365.

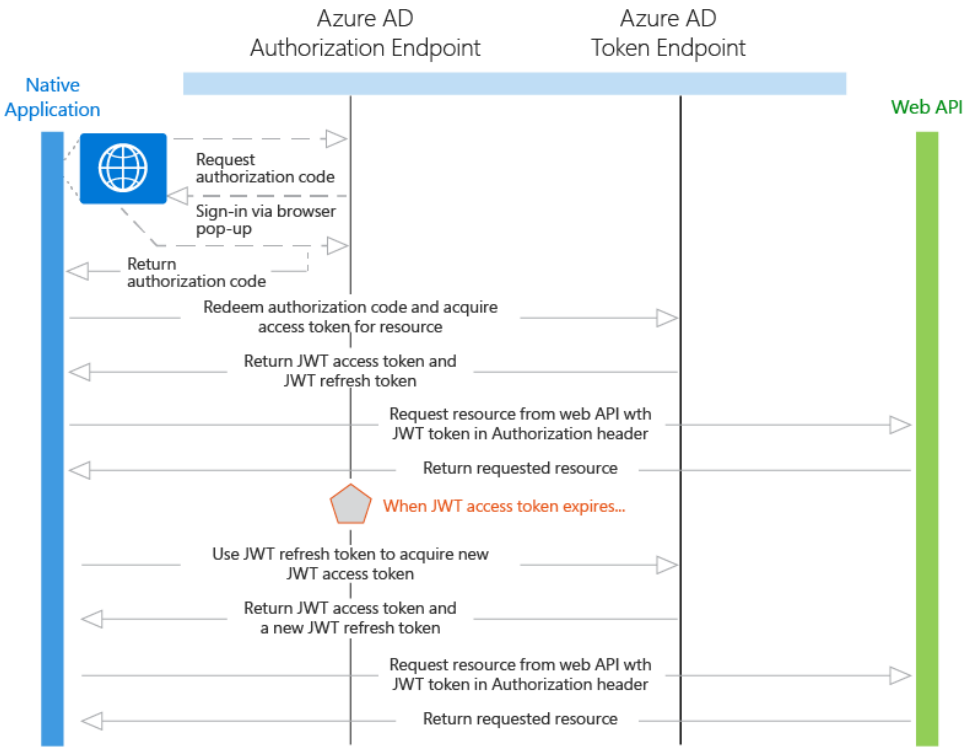
External Dependencies: Without exception, iPortalis have followed the Microsoft recommendations and procedures for enabling and performing secure interaction with the Client Office 365 related APIs.

Please refer to the following documentation for details on these recommendations:

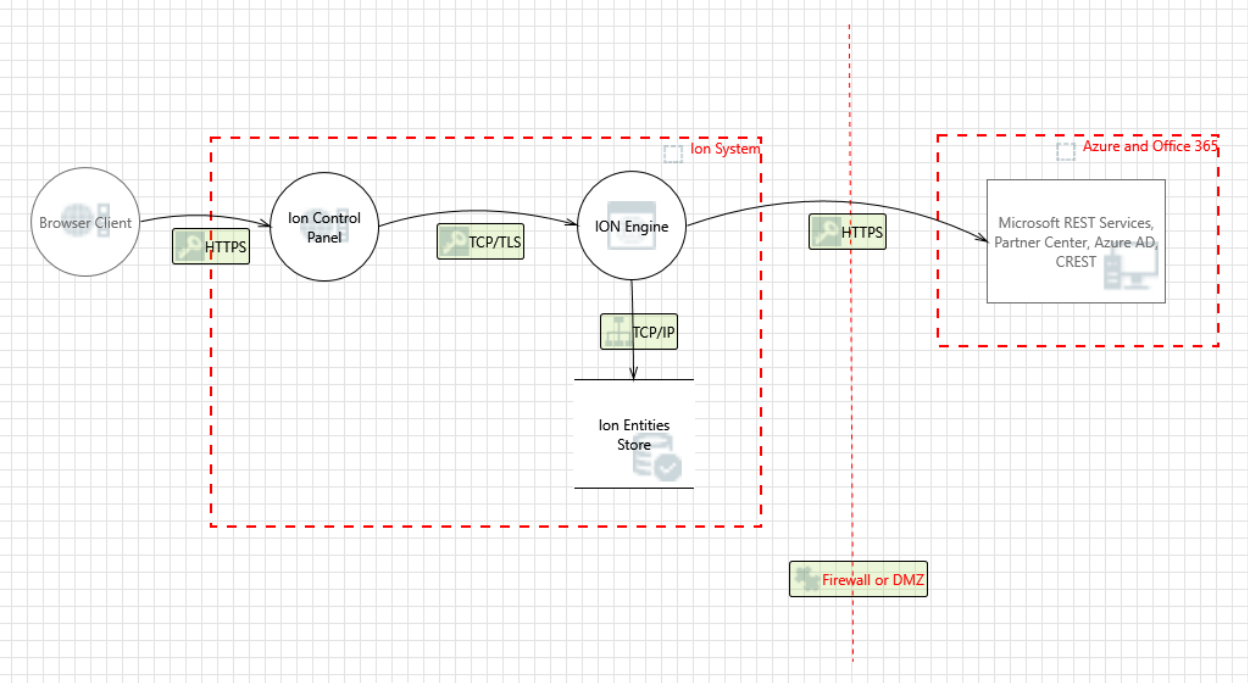
- https://support.office.com/en-us/article/Understanding-Office-365-identity-and-Azure-Active-Directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9
- https://support.office.com/en-us/article/Office-365-integration-with-on-premises-environments-263faf8d-aa21-428b-aed3-2021837a4b65?ui=en-US&rs=en-US&ad=US
- https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios
- https://msdn.microsoft.com/en-us/library/partnercenter/mt634709.aspx
- https://msdn.microsoft.com/en-us/library/partnercenter/mt709136.aspx
- https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications
- https://docs.microsoft.com/en-us/azure/app-service-mobile/app-service-mobile-how-to-configure-active-directory-authentication

The following diagrams illustrate the process flow of authentication:

Authentication Process Flow



Data Flow to Office 365



Threat(s) Not Associated with an Interaction

Data Flow HTTPS Is Potentially Interrupted

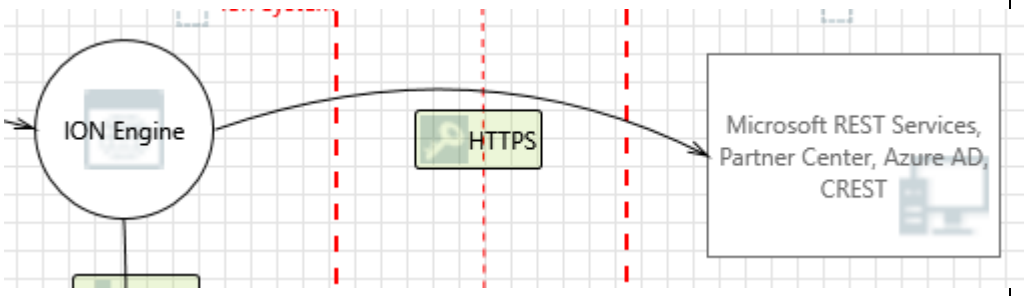
State:	Mitigation implemented
Priority:	High
Category:	Denial of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	Firewall or DMZ should be configured to prevent data flow interruption. If data flow is interrupted the provision process will fail, be logged with relevant information.

External Entity Microsoft Partner Center REST Service Potentially Denies Receiving Data

State:	Mitigation implemented
Priority:	High
Category:	Repudiation

Description:	Microsoft Partner Center REST Service claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	iCP engine provides an audit trail of any changes to entities and those requests that are made to the external services.

Spoofing of the Microsoft Partner Center REST Service External Destination Entity

State:	Mitigation implemented
Priority:	High
Category:	Spoofing
Description:	Microsoft Partner Center REST Service may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Microsoft Partner Center REST Service. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Threat is mitigated by requirement to provide symmetric secret and partner credentials.
Interaction:	HTTPS: 

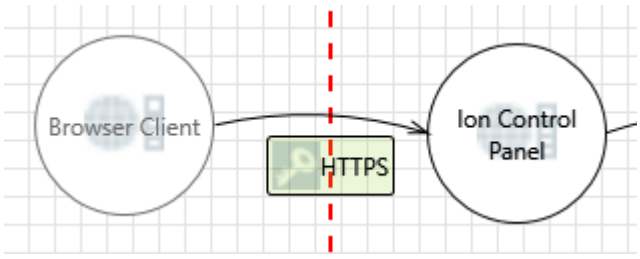
Data Flow HTTPS Is Potentially Interrupted

State:	Mitigation implemented
Priority:	High
Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	If data flow is interrupted, ION will fail the interaction and log the reason for failure. We expect the network perimeter to provider protection against DOS as well.

External Entity Microsoft REST Services, Partner Center, Azure AD, CREST Potentially Denies Receiving Data

State:	Mitigation implemented
Priority:	High
Category:	Repudiation
Description:	Microsoft REST Services, Partner Center, Azure AD, CREST claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	iCP engine audits any changes to entity store and also logs provisioning event failures or success.

Spoofing of the Microsoft REST Services, Partner Center, Azure AD, CREST External Destination Entity

State:	Mitigation implemented
Priority:	High
Category:	Spoofing
Description:	Microsoft REST Services, Partner Center, Azure AD, CREST may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Microsoft REST Services, Partner Center, Azure AD, CREST. Consider using a standard authentication mechanism to identify the external entity.
Justification:	A secret key, client id, and azure ad user credentials are required for this interaction. A secured and signed authentication token is acquired from the AD Azure service and used for subsequent operations. Capabilities of the user in office 365 is secured by their role in the office 365 tenant. That user is first authenticated through the control panel which authorizes against Azure AD and obtains the auth token which is passed down to the iCP engine.
Interaction:	HTTPS: 

Browser Client Process Memory Tampered

State:	Mitigation implemented
Priority:	High
Category:	Tampering
Description:	If Browser Client is given access to memory, such as shared memory or pointers, or is given the ability to control what Ion Control Panel executes (for example, passing back a function pointer.), then Browser Client can tamper with Ion Control Panel. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification:	The browser client is not given access to memory. The control panel is managed code.

Potential Data Repudiation by iCP

State:	Mitigation implemented
Priority:	High
Category:	Repudiation
Description:	iCP engine claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	iCP engine provides an audit trail for all changes to entities in the system.

Potential Process Crash or Stop for Ion Control Panel

State:	Mitigation implemented
Priority:	High
Category:	Denial Of Service
Description:	iCP engine crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification:	Control panel supports load balancing to ensure uptime.

Data Flow HTTPS Is Potentially Interrupted

State:	Mitigation implemented
Priority:	High
Category:	Denial Of Service
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	Authentication is required by an authorized entity. Retries for authentication is limited. To flood the system with request a compromise of authorized user credentials would be required. It is also expected that TCP/IP stack is hardened by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted. It is also recommended that you use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

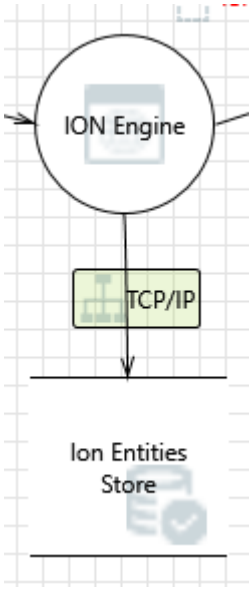
Elevation Using Impersonation

State:	Mitigation implemented
Priority:	High
Category:	Elevation of Privilege
Description:	iCP engine may be able to impersonate the context of Browser Client to gain additional privilege.
Justification:	Authentication is required by an authorized entity. Authenticated users are subject to restriction based on role based logic. The web service runs in an isolated application pool as network service which has almost no privileges on the local system. Input is validated to prevent buffer overflows. All interaction is with managed code.

iCP Engine May be Subject to Elevation of Privilege Using Remote Code Execution

State:	Mitigation implemented
Priority:	High
Category:	Elevation Of Privilege
Description:	Browser Client may be able to remotely execute code for iCP engine.
Justification:	Authentication is required by an authorized entity. The web service runs in an isolated application pool as network service which has almost no privileges on the local system. Input is validated to prevent buffer overflows. All interaction is with managed code.

Elevation by Changing the Execution Flow in Ion Control Panel

State:	Mitigation implemented
Priority:	High
Category:	Elevation Of Privilege
Description:	An attacker may pass data into Ion Control Panel to change the flow of program execution within Ion Control Panel to the attacker's choosing.
Justification:	Authentication is required by an authorized entity. The web service runs in an isolated application pool as network service which has almost no privileges on the local system. Input is validated to prevent buffer overflows. All interaction is with managed code.
Interaction:	TCP/IP 

Potential SQL Injection Vulnerability for Ion Entities Store

State:	Mitigation implemented
Priority:	High
Category:	Tampering
Description:	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
Justification:	Dynamic SQL statements are not constructed. Only parameterized queries to stored procedures are allowed. Customized reporting SQL only allowed by highest trust level.

Risks from Logging

State:	Mitigation implemented
Priority:	High
Category:	Tampering
Description:	Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, to reduce attack surface area. Be sure to understand and document log file elements which come from untrusted sources.
Justification:	Log files are stored in a proprietary xml format.

Spoofing of Destination Data Store Ion Entities Store

State:	Mitigation implemented
Priority:	High
Category:	Spoofing
Description:	iCP Entities Store may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of iCP Entities Store. Consider using a standard authentication mechanism to identify the destination data store.
Justification:	Data store is on secured network and access to connection data.

Lower Trusted Subject Updates Logs

State:	Mitigation implemented
Priority:	High
Category:	Repudiation
Description:	If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.
Justification:	Only highest trust level can log. Only the system does logging. External process or users not allowed to log.

Insufficient Auditing

State:	Mitigation implemented
Priority:	High
Category:	Repudiation
Description:	Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is such capture lightweight enough to be left on all the time? Do you have enough data to deal with repudiation claims? Make sure you log sufficient and appropriate data to handle a repudiation claims. You might want to talk to an audit expert as well as a privacy expert about your choice of data.
Justification:	Auditing is extensive.

Potential Weak Protections for Audit Data

State:	Mitigation implemented
Priority:	High
Category:	Repudiation
Description:	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure access to the log is through a reference monitor, which controls read and write separately. Document what filters, if any, readers can rely on, or writers should expect.
Justification:	Audit data is stored in entities data store and is protected by authentication and execution restrictions just as all other data.

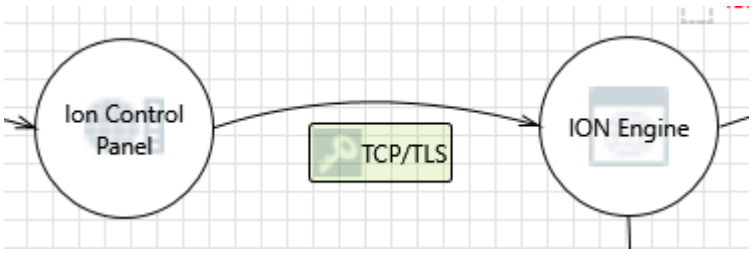
Authorization Bypass

State:	Mitigation implemented
Priority:	High
Category:	Information Disclosure
Description:	Can you access Ion Entities Store and bypass the permissions for the object? For example, by editing the files directly with a hex editor, or reaching it via file sharing? Ensure that your program is the only one that can access the data, and that all other subjects must use your interface.
Justification:	Data is restricted based on SQL identity. All changes are done via parameterized stored procedures. All other access is denied. Users can only access via control panel and access is restricted by role.

Weak Credential Storage

State:	Mitigation implemented
Priority:	High
Category:	Information Disclosure
Description:	Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a salted hash of the credentials instead of storing the credentials themselves. If this is not possible due to business requirements, be sure to encrypt the credentials before storage, using an SDL-approved mechanism. For client side, if storing credentials is required, encrypt them and protect the data store in which they're stored.
Justification:	Credentials are encrypted.

Potential Excessive Resource Consumption for iCP Engine or iCP Entities Store

State:	Mitigation implemented
Priority:	High
Category:	Denial of Service
Description:	Does iCP Engine or iCP Entities Store take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification:	Interaction between iCP engine and SQL Entities stored has been excessively tuned to prevent deadlocks and is currently operating in the field in many high demand environments. It is recommended that windows server and SQL server are tuned based on Microsoft recommendations.
Interaction:	TCP/TLS 

iCP Process Memory Tampered

State:	Not Applicable
Priority:	High
Category:	Tampering
Description:	If iCP is given access to memory, such as shared memory or pointers, or is given the ability to control what iCP Engine executes (for example, passing back a function pointer.), then iCP Control Panel can tamper with iCP Engine. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification:	Control is 100% managed code and has no access to memory.

Replay Attacks

State:	Not Applicable
Priority:	High
Category:	Tampering
Description:	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.
Justification:	Communication is managed code and this threat is mitigated by the TCP/IP stack. Application has no access to packets.

Collision Attacks

State:	Not Applicable
Priority:	High
Category:	Tampering
Description:	Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.
Justification:	Communication is managed code and this threat is mitigated by the TCP/IP stack. Application has no access to packets.

Weak Authentication Scheme

State:	Not Started
Priority:	High
Category:	Information Disclosure
Description:	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system. Consider the impact and potential mitigations for your custom authentication scheme.
Justification:	Active directory user account is required to submit requests to engine. Assuming the password policy on active directory is sufficiently strong, this threat is mitigated.

Elevation Using Impersonation

State:	Not Applicable
Priority:	High
Category:	Elevation of Privilege
Description:	iCP Engine may be able to impersonate the context of iCP to gain additional privilege.
Justification:	Not possible.

XML DTD and XSLT Processing

State:	Mitigation Implemented
Priority:	High
Category:	Tampering
Description:	If a dataflow contains XML, XML processing threats (DTD and XSLT code execution) may be exploited.
Justification:	Engine uses proprietary XML processing that does not allow DTD or XSLT code execution.

AD Properties Threat Modelling Report

AD Contact Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

AD Contact Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_DOMAIN_CONTROLLER	Selected Domain Controller	Selected Domain Controller	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD Container Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD Customer Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_DOMAIN_CONTROLLER_POOL	Selected Domain Controller Pool	The preferred domain controller	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

AD Customer Subscribed Service

Property Key	**Property Display Name**	**Property Description**	**Is Required**
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
MAX_CHILD_SUBSCRIBED_SERVICES_COUNT	Maximum Child Subscribed Service Count	The maximum number of subscribed services a customer can assign to child objects	No
SELECTED_DOMAIN_CONTROLLER	Selected Domain Controller	The preferred Domain Controller that has been assigned to the customer	Yes
SELECTED_LOCATION_REGION_DOMAIN_CONTROLLER	Selected Location Region Domain Controller	Selected Domain Controller for location regions	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD Domain Subscribed Service

Property Key	**Property Display Name**	**Property Description**	**Is Required**
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD Group Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

AD Group Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SAM_ACCOUNT_NAME	SAM Account Name	The SAM Account Name of the group.	No
SELECTED_DOMAIN_CONTROLLER	Selected Domain Controller	Selected Domain Controller	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD Resource User Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

AD Resource User Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SAM_ACCOUNT_NAME	SAM Account Name	The unique SAM Account Name given to the user	Yes
SELECTED_DOMAIN_CONTROLLER	Selected Domain Controller	Selected Domain Controller	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

AD User Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

AD User Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AD_OBJECT_DISTINGUISHED_NAME	AD Object Distinguished Name	The Active Directory objects Distinguished Name	No
AD_OBJECT_GUID	AD Object Guid	The Active Directory object Guid	No
AD_OBJECT_NAME	AD Object Name	The Active Directory Name for the Hosting object (normally Hosting)	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SAM_ACCOUNT_NAME	SAM Account Name	The unique SAM Account Name given to the user	Yes
SELECTED_DOMAIN_CONTROLLER	Selected Domain Controller	Selected Domain Controller	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

Preferred Domain Controller System Pool Item

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
IS_SHARED	Is Shared	Indicates whether the System Pool Item can be shared across multiple entities	Yes
MAX_ITEM_WEIGHT	Max Item Weight	The maximum about of resources value for this System Pool Item	Yes
PRIMARY_DOMAIN_CONTROLLER	Primary Domain Controller	The preferred Domain Controller that will be used for AD communication	Yes
SECONDARY_DOMAIN_CONTROLLER	Secondary Domain Controller	The secondary Domain Controller that will be used for AD communication if the primary Domain Controller cannot be contacted	No
SYSTEM_POOL_ITEM_KEY	System Pool Item Key	The unique key associated with the System Pool Item	Yes

O365 Properties Threat Modelling Report

Customer Offer

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
ENTITLEMENT_URI	Entitlement Uri	The entitlement uri	No
OFFER_QUANTITY	Offer Quantity	The quantity of seats for the offer	No
ORDER_ID	Order id	The Id of the order	No
SELECTED_MS_O365_OFFER	Selected offer	Selected Offer set for the company	Yes
SUBSCRIPTION_ID	Subscription Id	The Id of the subscription	No

Customer Offer Add On

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
ENTITLEMENT_URI	Entitlement Uri	The Microsoft default profile Id in Graph	No
OFFER_QUANTITY	Offer Quantity	The quantity of seats for the offer	No
SELECTED_MS_O365_OFFER_ADDON	Selected offer Addon	Selected Offer addon set for the company	Yes
SUBSCRIPTION_ID	Subscription Id	The Id of the subscription	No

Customer Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
COUNTRY_CODE	Country Code	The country code	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
LOCALE_CODE	Locale Code	The locale (culture) code	Yes
PROFILE_ID	Selected Profile	The profile selected for the plan	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

Customer Service Plan Offer

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_MS_O365_ADDONS	Selected Offer Addons	The selected offer addons	No
SELECTED_MS_O365_OFFER	Selected Offer	The selected offer	Yes

Customer Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
LANGUAGE_CODE	The Microsoft Tenant language code.	The Microsoft Tenant language code. e.g. en for English.	Yes
MAX_CHILD_SUBSCRIBED_SERVICES_COUNT	Maximum Child Subscribed Service Count	The maximum number of subscribed services a customer can assign to child objects	No
MS_O365_ADMIN_USER_PASSWORD	Admin User Password	The password for the admin user	No
MS_O365_ADMIN_USERNAME_PREFIX	Admin Username Prefix	The prefix for the admin username	No
MS_O365_COMMERCE_ID	Microsoft Customer Id	The Microsoft customer Id in Graph	No
MS_O365_DEFAULT_PROFILE_ID	Microsoft Default Profile Id	The Microsoft default profile Id in Graph	No
MS_O365_SYNC_DATE	O365 Sync Date	The date and time of the last sync	No
MS_O365_SYNC_ERROR	O365 Sync Error	The error message generated when the O365 sync fails	No
MS_O365_SYNC_STATUS	O365 Sync Status	The status of the Office 365 sync	No
MS_O365_TENANT_DOMAIN_PREFIX	The Microsoft Tenant domain name prefix.	The Microsoft Tenant domain name prefix.	No
MS_O365_TENANT_ID	Microsoft Tenant Id	The Microsoft tenant Id in Graph	No

SELECTED_MS_O365_PARTNER_PROFILE	Selected CSP Partner Profile	Selected CSP Partner Profile for the customer	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

Domain Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
AUTHENTICATION_TYPE	Authentication Type	The authentication type	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No
VERIFICATION_METHOD	Verification Method	The verification Method	Yes

Group Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
MAIL_ENABLED	Group is mail enabled	Group is mail enabled.	Yes
MAIL_NICKNAME	The Microsoft group mail nickname.	The Microsoft group mail nickname.	Yes
MICROSOFT_OBJECT_ID	Microsoft Object Id	The Microsoft object Id in Graph	No
SECURITY_ENABLED	Group is security enabled	Group is security enabled.	Yes
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

User Offer

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISABLED_MS_O365_OFFER_USER_SERVICES	Disabled user services	The disabled user services	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_MS_O365_OFFER	Selected offer	Selected Offer set for the company	Yes

Offer Add On

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_MS_O365_OFFER_ADDON	Selected offer Add on	Selected Offer addon set for the user	Yes

User Service Plan

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
AUTO_ADD_TO_ROOT_CUSTOMERS	Auto Add To Root Resellers	Auto Add To Root Customers	Yes
AUTO_ADD_TO_ROOT_RESELLERS	Auto Add To Root Resellers	Indicates if the service plan should be automatically added to a root resellers	Yes
BILLING_PRODUCT_CODE	Billing Product Code	The product code that can relate to a 3rd party billing package	No
COUNTRY_CODE	Country Code	The country code	Yes
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
LOCALE_CODE	Locale Code	The locale (culture) code	Yes
PROFILE_ID	Selected Profile	The profile selected for the plan	Yes
SERVICE_PLAN_BILLING_MODE	Service Plan Billing Mode	The billing mode of the service plan	Yes
SERVICE_PLAN_KEY	Service Plan Key	The unique key associated with the Service Plan	Yes
SPLA_DESCRIPTION	SPLA Description	The description of the SPLA	No
SPLA_NUMBER	SPLA Number	The SPLA Number associated with the Service Plan	No

User Service Plan Offer

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISABLED_MS_O365_OFFER_USER_SERVICES	Disabled user services	The disabled user services	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
SELECTED_MS_O365_ADDONS	Selected Offer Addons	The selected offer addons	No
SELECTED_MS_O365_OFFER	Selected Offer	The selected offer	Yes
SUBSCRIBER_EDITABLE	Subscriber Editable	Allow subscriber to change selected add ons and user services.	Yes

User Subscribed Service

Property Key	Property Display Name	Property Description	Is Required
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
MAIL_NICKNAME	The Microsoft user mail nickname.	The Microsoft user mail nickname.	Yes
MICROSOFT_OBJECT_ID	Microsoft Object Id	The Microsoft object Id in Graph	No
MICROSOFT_PASSWORD	Password for the new user.	The password for the new user	No
SERVICE_PLAN_KEY	Service Plan Key	The service plan key assigned to the subscriber	No

Subscriber Properties Threat Modelling Report

Contact

Property Key	Property Display Name	Property Description	Is Required
CITY	City	City	No
COMPANY_NAME	Company Name	The name of the company the contact belongs to	No
CONTACT_NAME	Contact Name	The name of the contact	-1
COUNTRY	Country	Country	No
COUNTRY_CODE	Country Code	Country Code	No
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DEPARTMENT	Department	Department	No
DESCRIPTION	Description	The description of the entity	No
DIRECT_REPORTS	Direct Reports	Direct Reports	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
EMAIL	Email	Email	No
EXTENSION_ATTRIBUTE_2	Extension Attribute 2	The AD Extension Attribute 2 Property	No
EXTENSION_ATTRIBUTE_3	Extension Attribute 3	The AD Extension Attribute 3 Property	No
EXTENSION_ATTRIBUTE_4	Extension Attribute 4	The AD Extension Attribute 4 Property	No
EXTENSION_ATTRIBUTE_5	Extension Attribute 5	The AD Extension Attribute 5 Property	No
FAX	Fax	Fax	No
FIRST_NAME	First Name	First Name	No
HOME_PHONE	Home Phone	Home Phone	No
INITIALS	Initials	Initials	No
IP_PHONE	IP Phone	IP Phone	No
LAST_NAME	Last Name	Last Name	No
MANAGER	Manager	Manager	No
MOBILE_PHONE	Mobile Phone	Mobile Phone	No
NOTES	Notes	Notes	No
OFFICE	Office	Office	No
PAGER	Pager	Pager	No
PARENT_COMPANY_CONTAINER	Parent Company Container	The parent company container	No
SECURITY_ROLE_SCOPE	Security Role Scope	The security scope for the given subscriber	No
STATE	State	State	No
STREET	Street	Street	No
SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No
TITLE	Title	Title	No
WEB_PAGE	Web Page	Web Page	No
WORK_PHONE	Work Phone	Work Phone	No
ZIPCODE	Zip Code	Zip Code	No

Customer

Property Key	Property Display Name	Property Description	Is Required
AFFILIATED_RESELLER	Affiliated Reseller	The name of the affiliated reseller	No
ALLOW_USERS_ADMIN_RIGHTS	Allow users administration rights	Tells the system if users (not admins) in the company are allowed to use the control panel	No
ALLOW_USERS_CHANGE_GROUP	Allow users Change Group Membership	Tells the system if users (not admins) in the company are allowed to change group membership	No

ALLOW_USERS_CHANGE_PASSWORD	Allow users change password	Tells the system if users (not admins) in the company are allowed to change their own password	No
ALLOW_USERS_CHANGE_PLAN	Allow users Change Plan	Tells the system if users (not admins) in the company are allowed to change plan settings for themselves	No
BUSINESS_SECTOR	Business Sector	The business sector the customer belongs too	Yes
CHALLENGE_QUESTION_REQUIRED	Challenge Question Required	Tells the system if users (not admins) in the company are required to have a challenge question	No
CITY	City	City	No
CONTACT_EMAIL	Contact Email	The email address of the main contact for the company	No
CONTACT_NAME	Contact name	The CN name of the main contact for the company	No
CONTACT_PHONE	Contact Phone	The phone number of the main contact for the company	No
COUNTRY	Country	Country	No
COUNTRY_CODE	Country Code	The country code of the customers address	No
CULTURE_CODE	Culture code	The culture code assigned to this company	Yes
CUSTOMER_ACCOUNT_NUMBER	Customer Account Number	An external account number for the customer to tie in with 3rd party systems	No
CUSTOMER_CODE	Customer Code	Unique Code of the customer	Yes
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
PASSWORD_STRENGTH	Password Strength	The password strength that is enforced for the company	No
REASON_FOR_CANCEL	Reason for Cancel	The reason given for cancelling service	No
SALES_PERSON	Sales Person	The name of the sales person	No
SECURITY_ROLE_SCOPE	Security Role Scope	The security scope for the given subscriber	No
SIGNUP_DOMAIN	Reseller Signup domain	The domain the customer entered into the system through (the resellers domain)	Yes
STATE	State	State	No
STREET	Street	Street	No
SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No
TRIAL_ACCOUNT	Trial Account	Tells the system if this customer is a trial (Demo) customer	Yes
TRIAL_END_DATE	Trial End Date	The date the trial service is over	No
TWO_STEP_AUTH_REQUIRED	Two Step Authorization Required	Tells the system if two step authorization is required.	Yes
ZIPCODE	Zip Code	Zip Code	No

DOMAIN

Property Key	Property Display Name	Property Description	Is Required
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
DNS_HOST	DNS HOST	DNS Hoster that the DNS is stored at	No
DOMAIN_NAME	Domain Name	The name of the domain	Yes
IS_SHARED	Is Shared	If this is a shared domain	Yes
MAIL_IP_ID	Mail IP ID	Mail IP ID	No
OWA_SUB_DOMAIN	OWA Sub domain	OWA Sub domain entry point into the system	No
REGISTRAR	Registrar	Registrar	No
SUB_DOMAIN	Sub domain	Sub domain entry point into the system.	No

SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No
WWW_IP_ID	Sub domain	Sub domain	No

GROUP

Property Key	Property Display Name	Property Description	Is Required
AUTOMATIC_USER_MEMBERSHIP	Automatic User membership	Automatically adds a new user to the groups membership	Yes
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DESCRIPTION	Description	The description of the entity	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
EMAIL	Email	Email	No
EXTENSION_ATTRIBUTE_2	Extension Attribute 2	The AD Extension Attribute 2 Property	No
EXTENSION_ATTRIBUTE_3	Extension Attribute 3	The AD Extension Attribute 3 Property	No
EXTENSION_ATTRIBUTE_4	Extension Attribute 4	The AD Extension Attribute 4 Property	No
EXTENSION_ATTRIBUTE_5	Extension Attribute 5	The AD Extension Attribute 5 Property	No
GROUP_NAME	Group Name	The name of the group	Yes
GROUP_SCOPE	Group Scope	The scope of the group	Yes
GROUP_TYPE	Group Type	The type of the group	Yes
MANAGED_BY	Managed By	The manager of the group	No
PARENT_COMPANY_CONTAINER	Parent Company Container	The parent company container	No
SECURITY_ROLE_SCOPE	Security Role Scope	The security scope for the given subscriber	No
SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No

RESOURCE USER

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_SECURITY_ROLE_GROUP	Assigned Security Role Group	The security group for the given user	No
CHALLENGE_MESSAGE	Challenge Message	Challenge Message	No
CHALLENGE_RESPONSE	Challenge Response	Challenge Response	No
CITY	City	City	No
COMPANY_NAME	Company Name	The company a user is associated with	No
COUNTRY	Country	Country	No
COUNTRY_CODE	Country Code	Country Code	No
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DEMO_ACCOUNT	Demo Account	Tells the system if this user is a Demo user, not to be billed	Yes
DEPARTMENT	Department	Department	No
DESCRIPTION	Description	The description of the entity	No
DIRECT_REPORTS	Direct Reports	Direct Reports	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
EMAIL	Email	Email	No
EXTENSION_ATTRIBUTE_2	Extension Attribute 2	The AD Extension Attribute 2 Property	No
EXTENSION_ATTRIBUTE_3	Extension Attribute 3	The AD Extension Attribute 3 Property	No
EXTENSION_ATTRIBUTE_4	Extension Attribute 4	The AD Extension Attribute 4 Property	No
EXTENSION_ATTRIBUTE_5	Extension Attribute 5	The AD Extension Attribute 5 Property	No

FAX	Fax	Fax	No
FIRST_NAME	First Name	First Name	No
HOME_PHONE	Home Phone	Home Phone	No
INITIALS	Initials	Initials	No
IP_PHONE	IP Phone	IP Phone	No
LAST_NAME	Last Name	Last Name	No
MANAGER	Manager	Manager	No
MOBILE_PHONE	Mobile Phone	Mobile Phone	No
NOTES	Notes	Notes	No
OFFICE	Office	Office	No
PAGER	Pager	Pager	No
PARENT_COMPANY_CONTAINER	Parent Company Container	The parent company container	No
PASSWORD_NEVER_EXPIRES	Password Never Expires	The users password never expires	Yes
RESOURCE_USER_TYPE	Resource User Type	The type of resource user	Yes
SECURITY_ROLE_SCOPE	Security Role Scope	The security scope for the given subscriber	No
STATE	State	State	No
STREET	Street	Street	No
SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No
TITLE	Title	Title	No
UNLOCK_ACCOUNT	Unlock Account	Indicates if the users account should be unlocked	Yes
USER_CANNOT_CHANGE_PASSWORD	User Cannot Change Password	The user cannot change their password	Yes
USER_MUST_CHANGE_PASSWORD	User Must Change Password	The user must change their password	Yes
USER_PASSWORD	User Password	The users password	No
USER_PRINCIPAL_NAME	User Principal Name	The unique UPN given to the user	Yes
USER_ROLE_KEY	User Role Key	The security role assigned to the user	Yes
WEB_PAGE	Web Page	Web Page	No
WORK_PHONE	Work Phone	Work Phone	No
ZIPCODE	Zip Code	Zip Code	No

USER

Property Key	Property Display Name	Property Description	Is Required
ASSIGNED_SECURITY_ROLE_GROUP	Assigned Security Role Group	The security group for the given user	No
CHALLENGE_MESSAGE	Challenge Message	Challenge Message	No
CHALLENGE_RESPONSE	Challenge Response	Challenge Response	No
CITY	City	City	No
COMPANY_NAME	Company Name	The company a user is associated with	No
COUNTRY	Country	Country	No
COUNTRY_CODE	Country Code	Country Code	No
DEFAULT_LOCATION_REGION	Selected Location Region	The location region assigned to the user	No
DEMO_ACCOUNT	Demo Account	Tells the system if this user is a Demo user, not to be billed	Yes
DEPARTMENT	Department	Department	No
DESCRIPTION	Description	The description of the entity	No
DIRECT_REPORTS	Direct Reports	Direct Reports	No
DISPLAY_NAME	Display Name	The display name for the entity	Yes
EMAIL	Email	Email	No

EXTENSION_ATTRIBUTE_2	Extension Attribute 2	The AD Extension Attribute 2 Property	No
EXTENSION_ATTRIBUTE_3	Extension Attribute 3	The AD Extension Attribute 3 Property	No
EXTENSION_ATTRIBUTE_4	Extension Attribute 4	The AD Extension Attribute 4 Property	No
EXTENSION_ATTRIBUTE_5	Extension Attribute 5	The AD Extension Attrubute 5 Property	No
FAX	Fax	Fax	No
FIRST_NAME	First Name	First Name	No
HOME_PHONE	Home Phone	Home Phone	No
INITIALS	Initials	Initials	No
IP_PHONE	IP Phone	IP Phone	No
LAST_NAME	Last Name	Last Name	No
MANAGER	Manager	Manager	No
MOBILE_PHONE	Mobile Phone	Mobile Phone	No
NOTES	Notes	Notes	No
OFFICE	Office	Office	No
PAGER	Pager	Pager	No
PARENT_COMPANY_CONTAINER	Parent Company Container	The parent company container	No
PASSWORD_NEVER_EXPIRES	Password Never Expires	The users password never expires	Yes
SECURITY_ROLE_SCOPE	Security Role Scope	The security scope for the given subscriber	No
STATE	State	State	No
STREET	Street	Street	No
SUBSCRIBED_SERVICE_KEYS	Subscribed Service Keys	The service keys the subscriber is subscribed to	No
TITLE	Title	Title	No
UNLOCK_ACCOUNT	Unlock Account	Indicates if the users account should be unlocked	Yes
USER_CANNOT_CHANGE_PASSWORD	User Cannot Change Password	The user cannot change their password	Yes
USER_MUST_CHANGE_PASSWORD	User Must Change Password	The user must change their password	Yes
USER_PASSWORD	User Password	The users password	No
USER_PRINCIPAL_NAME	User Principal Name	The unique UPN given to the user	Yes
USER_ROLE_KEY	User Role Key	The security role assigned to the user	Yes
WEB_PAGE	Web Page	Web Page	No
WORK_PHONE	Work Phone	Work Phone	No
ZIPCODE	Zip Code	Zip Code	No

Information Storage

What Information is Stored

iCP store almost identical data for an on premise system (e.g. Skype, Active Directory, etc.) as for office 365. This includes things like company and user properties (names, addresses, etc.), settings for a specific service, group membership, etc.

If the data is sensitive, such as passwords, it is encrypted in our database as standard. Important: any data entity property can be encrypted upon request.

For Office 365 specifically, iCP also store entitlements such as what subscriptions the customer has, number of licenses per subscription, who licenses are assigned to, the details of offerings, and the service plan components of a given offer. Office365 itself stores a lot of data, but that is out of iCP scope.

Where is Information Stored

All office 365 specific data is stored in iCP Microsoft SQL Server Entities database. The system as a whole stores data either in Entities database or in the Configuration database. There is a small amount of system level information stored in XML configuration files and in some secured registry settings. Finally, if using iCP Dir Sync solution, AD changes are temporary stored in an additional SQL database until those changes are sync'd to iCP system.

How Long is Information Stored

Information is stored "indefinitely" as even deleted objects are simply flagged as deleted and kept in the Entities DB. This can be adjusted and controlled further by Client IT administration.

As mentioned earlier the Dir Sync database only keeps data until the synchronization is complete.

How Accessible is Information

The data is on a back-end SQL Server, on-premise and within the Client network. It has very limited access, and the database itself is secured with a service account password and data access is performed via stored procedures.

Who Can Access Information

All other access is via either the iCP or APIs that require authentication. Users are also limited in what they can do via their security role such as an administrator or a standard user. (Defined by Client).

Administration Layers

This refers to a security model that identifies the rights of each actor (e.g. user/role) with respect to objects/data stored in iCP. This has been characterized from a high-level above and in the threat model.

iCP version 7.0 is in development roadmap and iPortalis are adding increased control measures around authorization and user roles. The iCP current model consists of:

- Domain Admin
- Hosting Admin
- Hosting CSR
- Reseller Admin
- Reseller CSR
- Company Admin
- Company User