Sertainty UXP Technology

Core Components Guide

V3.6.0

Copyright 2021, Sertainty Corporation

Table of Contents

1 Introduction to the Sertainty UXP Core Components

Sertainty UXP Technology implements the Unbreakable Exchange Protocol (UXP). This protocol provides a methodology to protect and control access to sensitive data.

The core entity in UXP Technology is the UXP Object. The UXP Object is a portable protocol used to protect data in a self-managed, one-of-a-kind entity. UXP Technology blends proprietary UXP Intelligence and a unique protection scheme with any size dataset. The result is a UXP Object.

Empowered with UXP Technology, the UXP Object self-protects and self-governs its own access and mitigation activity. These activities are defined by the data-owner using the owner's pre-determined ruleset.

Additionally, throughout UXP Technology are role-based, special purpose UXP Objects. These Objects are protected by UXP Technology, and each perform a specific role within UXP Technology. These Objects are discussed in subsequent guides.

Once UXP Technology is integrated into a third-party application, the application is now referred to as a UXP Object-aware application.

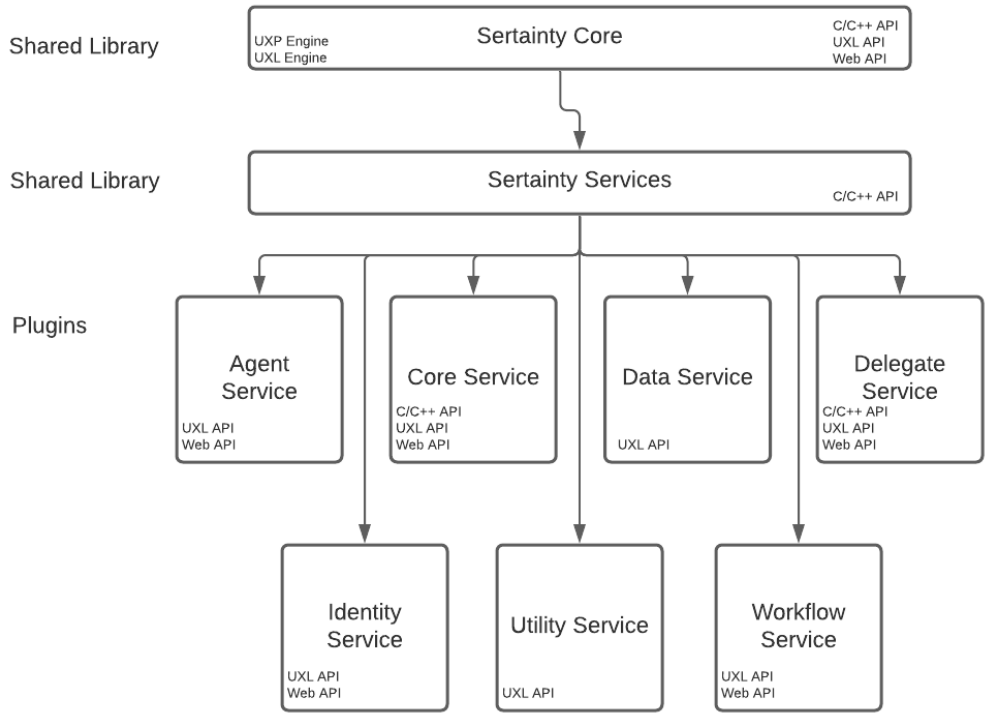

Figure 1 - Core Architecture Overview

2 UXP Object

UXP Object is the universal term used for the result when data is protected using UXP Technology. Throughout the documentation, this entity is referred to as an Object, and occasionally as a “UXP”.

As mentioned in the Section 1 above, the UXP Object is a portable protocol used to protect data in a self-managed, one-of-a-kind entity. In Object form, the embedded UXP Intelligence and unique protection scheme allow the Object to protect and govern its own access and mitigation activity.

Once a UXP Object is created, it appears as an inert, binary file showing a ***.uxp** extension. The UXP Object is unidentifiable unless proximal to UXP Technology. Without proximity, a UXP Object simply looks ordinary and nondescript on any OS.

UXP Object Generation: A UXP Object is generated from a special-purpose Object called the UXP Identity. The Identity contains essential access and mitigation attributes along with a list of permitted User(s) and their unique details. These attributes and details are also used to build the protection scheme for the Object. The Object must contain a valid UXP Identity that includes at least *one active User* (also referred to as a *User Definition*). Multiple Users can be in a UXP Identity. Without an active User, the UXP Object will be inaccessible and permanently locked.

Internal Components: All UXP Objects contain specific internal core components. Each component serves an essential purpose for the overall function of the Object.

The components are listed below:

- KCL Code
- Virtual Header File
- Internal Metadata
- Virtual File System

2.1 KCL Code

The KCL Code is a light-weight p-code executable operating very similarly to a conventional computer. As an executable embedded in the UXP Object, this UXP proprietary program is written in a C-like language and serves as the Object’s Intelligence Engine.

As an executable, the KCL Code requires proximity to UXP Technology, specifically the *external UXP Engine*. *The UXP Engine provides the executable environment for the KCL Code*. Otherwise, the KCL Code sits dormant and undetectable in the inert UXP Object.

The UXP Engine in discussed in the *UXP Core Technology Construction Guide* (currently being edited).

The KCL Code originates from the UXP Identity. Within the Identity, the KCL Code consists of access and mitigation rules and User Definitions (section 3.3.1). Rules and User Definitions are artifacts defined by the data owner.

The Identity is discussed in Section 3 below.

Unique to each Object, the KCL Code is fully self-contained and OS agnostic. These two characteristics allow the KCL Code to run the same compiled KCL Code on all supported platforms without modification or re-compilation.

The KCL Code is discussed fully in the *UXP KCL Guide*.

2.1.1 KCL Functions

UXP Object Creation: During the Object's creation process, the KCL Code is also integral in the UXP Object's encryption key generation. These keys are randomly generated by the UXP Engine, another proprietary engine external to the Object.

Key Management: Additionally, the KCL Code manages all encryption keys internally throughout the Object's life cycle. Keys are embedded unseen in the Object and protected using a proprietary, recursive UXP Protection Scheme.

Intelligent Decision-Maker: During an Object authentication attempt, the KCL Code, containing Rules and User Definition(s), acts as a decision-maker. When a User (human, machine, or process) attempts to authenticate, the KCL Code evaluates all relevant information.

This information includes the following:

- Rules and User Definition(s) within the KCL Code provided by the data owner
- Environmental information collected externally by the UXP Technology proprietary process.

The information within the KCL Code must match the external environment for a successful access. If the KCL Code denies access, the potential User will never access the protected data within the UXP Object.

2.1.2 KCL Origins

The KCL Code can be constructed two ways:

- **Custom KCL**

  KCL is a proprietary C-like language. This language provides a flexible way of constructing the KCL Code program. It does, however, require programming skills and can be challenging to implement. The benefit of using custom KCL Code is that a developer can implement decisions unique to the implementation.

The KCL Code is discussed fully in the *UXP KCL Guide*.

- **UXP Identity**

  The easier and preferred method for constructing KCL Code is using the UXP Identity. The KCL Code is constructed automatically when an Identity is generated using a proprietary process. Prior to the process, the data owner defines the necessary artifacts, Rules and User Definitions. These artifacts along with UXP Metadata are used to automatically generate the KCL Code. The benefit is that the data owner/developer can create KCL Code without writing the KCL Code module**.**

  The UXP Identity is discussed in Section 3 below.

2.2 Virtual Header

Every UXP Object contains a Virtual Header that allows the external UXP Engine to identify the Object as a valid entity. If a Header can't be found or read, then the Object isn't considered a valid UXP Object.

The Virtual Header is uniquely identified using a security domain consisting of multiple tokens. By default, the UXP Engine provides a default set of tokens. This default token set allows any UXP Object created to be recognized by all other installations of UXP Technology.

If a particular installation prefers a private UXP Object format, a domain can be defined and used when creating and accessing Objects. If the correct security domain information isn't provided when opening the Object, the UXP Engine will be unable to access the Virtual Header information. The immediate mitigating result is that the Engine will terminate the operation.

Security Domain: A security domain has two forms, dynamic and fixed. Both forms are considered private domains within UXP Technology.

- **Dynamic**

  A dynamic security domain is private to the user of UXP Technology. This domain information consists of a two-part key. The two parts of this key are a 32-character key and a number between 2 and 127. This key information is defined by the user prior to Object creation; the information isn't auto-generated. Once defined, the user is responsible for the two-part key management and protection.

  The process or person will need to know and remember the domain in order to access the UXP Object.

  The dynamic domain is assigned when the UXP Object is created. The two-part key, if necessary, can be reused for future Object creation.

  If a dynamic security domain is being used and the user accessing the Object ISN'T the definer or creator of this domain, then the two-part key must be shared. It is recommended to not share this information in the clear.

- **Fixed**

  A fixed security domain contains a two-part key, but unlike the dynamic domain, this information is embedded in the Sertainty License. Also, the Sertainty team sets up the License using a proprietary process.

  A fixed domain form can't be modified. Since the License manages the fixed domain, the user only needs to indicate the desired domain when creating a UXP Object. To open a UXP Object that uses a Licensed fixed domain, the external UXP Engine will automatically identify the License domain and use that information to access the UXP Object.

  If the fixed domain defined in the UXP Object doesn't match the License, then the UXP Object isn't recognized as a valid UXP Object. Access to the Object is denied.

2.3 Internal Metadata

The internal metadata specific to a UXP Object contains all the virtual file system data. All other user-specific data is stored as virtual data files.

2.4 Virtual File System (VFS)

All artifacts within the UXP Object are stored as virtual files.

Private cloaking keys protect a virtual file.

2.4.1 Description

A virtual file is very similar to a typical file on disk, except that a virtual file is encapsulated within the defined UXP Object. The virtual file content is identical to its physical counterpart. However, several transparent permutations may occur while transferring data into the protected UXP Object. These permutations are discussed below:

- Data is divided into fixed-length pages that are indexed. The page size can be specified at import time, or the page size can be defaulted. In both cases, the page size value is always aligned to the nearest power of two that is greater than or equal to the specified value. The default value is 2MB.

  > **Example:** If a video file has a page size of 2MB, yet the user application is fetching 512-byte buffers, then the caching system will avoid a hard disk fetch by reading the requested data from an in-memory buffer. For random access, the caching provides little benefit.

- At creation time, the virtual file can optionally be compressed. Depending on the file contents, compression can reduce virtual file sizes up to 90%.

- A proprietary cloaking algorithm, based on industry standard encryption and other cloaking techniques, protects all data. An added outcome using this algorithm with the VFS is that most data artifacts are protected multiple times via a recursive I/O system.
- The data can be hidden within the UXP Object by prefixing the virtual file or directory name with a "." character. Only Users with owner privileges can access hidden virtual files.

2.4.2 Management Structure

When a virtual file is created within a UXP Object**,** the data within the file is managed similarly to a conventional file system. The VFS can maintain a hierarchy of directory structures, where each may contain virtual files and sub-directories.

2.4.3 Structure

A virtual file is identified by its full directory path and name.

In a virtual file path, a directory separator is the forward slash. The top-most directory is ***/***.

> **Example:** A simple virtual file name **TMP** at the top level would have a full path name of **/TMP**. The same virtual file within a sub-directory **MyDir** would have a full path name of **/MyDir/TMP**.

Virtual names must be represented using the following criteria:

- Unique within their current directory.
- At least one non-blank character in length.

The VFS can support an entire directory hierarchy within a UXP Object.

2.4.4 Encryption and Cloaking Keys

All the encryption and cloaking keys created for a single UXP Object are stored within the VFS of the UXP Object.

2.4.5 User Data

User data can be any block of data.

> **Note:** User data isn't required in UXP Object.

The internal core components for the UXP Object can be generated without user data.

The UXP Engine accepts serializable objects, string data, binary data, and files to produce a protected entity within the UXP Object. To the UXP Engine, data is always treated as a series of unsigned bytes that can contain any value.

The UXP Engine can protect a single data artifact or many artifacts concurrently. Additionally, the UXP Engine has a built-in Virtual File System that will permit a complete file hierarchy to be protected within a single instance of a UXP Object.

2.4.6 User Data Types

Data can be any user-specified type, such as *.mp4, *.mp3, *.txt, etc. The virtual file can originate from either an existing file or an in-memory buffer. The Virtual File System can contain anything that can normally go into a conventional file system. The VFS is only limited in size by the operating system itself.

3 UXP Identity

A UXP Identity plays a central role in UXP Technology. The Identity is more than a username and password set; it extends beyond the traditional definition of a digital identity.

The Identity is a special purpose UXP Object that is secured using the same protection scheme as a UXP Object. The UXP Identity differs from the UXP Object in the two ways mentioned below:

- The content in the Identity can't be edited.
- The Identity contains no customer data.

A UXP Identity can represent a single User or a group of Users (Workgroup). To have a Workgroup, each User in the group must have their own, individual UXP Identity prior to creating a Workgroup Identity. Specific *private attributes* from each individual Identity are required to generate a Workgroup Identity.

A User in an Identity can represent a *human*, *machine or process*. A Workgroup Identity can be any combination of human, machine or process.

Single-User and Workgroup UXP Identities are generated in the same way.

3.1 Function

The UXP Identity contains and protects the components that permit the UXP Object to be intelligent and proactive. Once a UXP Object is authenticated, the Identity continues securing the Object while the data is in-use.

The UXP Identity is required to generate a UXP Object. In a protected file format, the Identity houses the owner-specified access and mitigation Rules and a list of permitted Users for a dataset. These Rules and User list (*together referred to as owner-defined artifacts*) are required to create the unique protection scheme within the UXP Object.

3.2 Format

The UXP Identity originates from an *.xml file called the **ID Definition XML**. This XML is the UXP Identity's "source code" and can be defined and managed using the following methods:

- Custom development using an ID Definition XML template. The template is provided with the UXP Technology Kit and also be accessed from the Developer Portal.
- Custom KCL Code (*see Sertainty UXP KCL Guide for more detail*)

The ID Definition content and its corresponding XML are discussed in sections 3.3.

The ID Definition XML requires being compiled before the XML can be executed. UXP Technology has a specific process for publishing the XML to a file format. The publication process incorporates additional UXP Metadata needed by UXP Technology to execute the UXP Identity functions mentioned in section 3.1. The *published ID Definition XML* is now the UXP Identity in a file format. In Identity file format, the XML content is unseen and can no longer be edited.

As a UXP Identity, the file appears as an inert, binary showing an ***.iic** extension. This *.iic file type is unidentifiable unless proximal to UXP Technology libraries. It looks ordinary and nondescript on any O/S and can be easily designated as junk.

A UXP Identity is fully protected using UXP Technology. No access parameters (Rules, Users*) or other XML attributes are seen or referred to in any way. These attributes along with additional unseen UXP Metadata provide verification details used by UXP Technology at the time when the UXP Identity is used to protect a dataset.

> ***Note**: The ID Definition XML does contain some public information attributes that are unrelated to access. The public information is basic, obvious content. Though this content is public, it is also used in the protection scheme for the UXP Identity and any UXP Object's created using this Identity. These public attributes are Identity-Level and User-Level. Both levels are discussed in sections below.

3.3 ID Definition XML: UXP Identity Source Document

The UXP Identity used to protect data in a UXP Object now contains the executable that governs that UXP Object's activity. The content for the executable originates from a source document specific to UXP Technology called the **ID Definition XML**.

The ID Definition content is defined and managed in the ID Definition XML.

The ID Definition XML is a template containing the required and optional attributes for creating a UXP Identity. This template lists the attributes in the required hierarchy for a successful publication.

Most blocks don't require all attributes listed if they *aren't* populated for a successful publication.

The ID Definition XML document is named at the owner/creator's discretion.

3.3.1 Content and Structure

Owned-defined artifacts provide the attributes for the ID Definition content. There are two types of attributes: *public* and *private*. Also, there are *two levels of public and private attributes* within the ID Definition. The two levels are *Identity-Level* (ID-Level) and *User-Level**.

> ***Note**: Most User-Level attributes are defined in a separate process prior to populating the ID Definition XML. This process occurrence is dependent upon the types (*human, machine, process*) of User(s) to be included in the XML. The User-Level attributes are collected as a UXP-specific subcomponent called the **User Definition**. The User Definition is discussed below somewhere.

The ID Definition XML is structured into the three primary blocks, or sections. The Users section is further sub-sectioned. The blocks are listed below:

- **Public information** – This section isn't specifically titled using this phrase, but the section is the beginning of the XML with the first attribute being the ID name.
- **Rules** – These are the ID-Level Rule blocks and are private information.
- **Users**
  - **User** – This section is contains the User Definition credential set. In a Workgroup Identity, each User will have their own block containing the sections below.
    - **Public information** – This section isn't specifically titled using this phrase, but the section is the beginning of the User block with the first attribute being the User name.
    - **Private** – This section shows these attributes in their entirety if the User is the Identity owner or someone who has control over the credentials in the User Definition. However, if an Identity is being created on behalf of another User, the User's private attributes will be encrypted within the XML. These attributes are cloaked and hidden once the ID Definition XML is published. Examples are provided Appendix A.
      - **Rules** – These Rule blocks are defined by and known only to this User. They are access-specific for that User only.
      - **Challenge Pairs** – These are the Prompt/Response sets utilized for authentication. They are private to each User.
- Rules – These are User-Level Rule blocks that can be defined by the Identity owner. Once the ID Definition is published, these are cloaked.

3.3.2 Publishing

The ID Definition XML requires, at a minimum, the following attributes to successfully be published as a UXP Identity file:

- ID name
- Expiration date
- One ID Privilege defined (see section 3.3.3.1)
- One *User Definition* credential set
  - User public information
  - One User-Level Privilege
  - Challenge Pairs

If no Rules are defined, UXP Technology will use default settings when publishing the ID Definition XML to a UXP Identity file. The UXP Technology default Rule settings are system generated for the XML and include minimum access requirements. The system default requirement is presenting three Challenge Pairs during authentication.

These default settings are inaccessible, but the settings can be overridden in one of two ways:

- The first option is by defining a separate customized Rule Preset XML if a custom default setting is needed. This XML uses the same the ID Definition XML template to define Rules that can represent the desired default settings. Rule Preset XML is discussed further in Rules section somewhere below.
- The other option to update the default settings is to populate individual Rule blocks in the ID Definition XML and re-publish the XML to a UXP Identity file.

3.3.3 ID Definition Attributes

ID Definition attributes are organized into following three blocks or sections:

- Public information
- Rules
- Users

3.3.3.1 Public Information

The public information attributes are a collection of descriptive details associated to traditional information. Along with this information, there are specific *UXP Identity Privileges* defining the permitted usage of the Identity once the ID Definition XML is published to a UXP Identity. These Privileges along with the public information attributes are described in Table 1.

Table 1. Public Attributes in the ID Definition XML

Public Attribute	Datatype	Description
ID name	Name	This name is the name of the UXP Identity when the ID Definition XML is published. It isn't necessarily the name of the Identity owner. The ID name issued is discretionary to the Identity owner/creator. **Required**
Description	String	Description is a discretionary statement to define or describe the use of this Identity. **Optional**
Expiration	Date	Expiration is the date and time when the Identity is no longer valid. Year-Month-DayThour:minute:seconds **Example**: 2121-02-15T18:30:00 The *hour* in the time is measured 0-24. If no date and time populates this attribute OR a zero value is defined when the ID Definition XML is published, a default date and time is assigned. **Default**: 100 years from the date of publication **Required*** ***Note**: To prevent getting around this date using time manipulation methods, an additional *Untrusted Time Restriction* attribute can be defined. Section 3.3.4.2.11
PersonalName1	String	Name of the Identity owner/creator or permitted User in the Identity. **Optional**

Public Attribute	Datatype	Description
PersonalName2	String	Name of the Identity owner/creator or permitted User in the Identity. **Optional**
PersonalName3	String	Name of the Identity owner/creator or permitted User in the Identity. **Optional**
Address1	String	Physical address or location information **Optional**
Address2	String	Physical address or location information **Optional**
City	String	**Optional**
State	String	**Optional**
Zipcode	String	**Optional**
Country	String	**Optional**
Privileges	String	These Privileges define *HOW* this Identity is to be used. They are unrelated to how the UXP Object will behave. Only the Rules impact the behavior of the UXP Object. The bolded words are the actual values available. **Files**: Permits Identity to create UXP Objects **Messages**: Permits Identity to create a SmartMessage **SSO**: Permits Identity to start a Single-Sign-On session

Public Attribute	Datatype	Description
		Imports: Permits a User Definition that is published in a UXP Identity to be imported into another ID Definition. One Privilege is **REQUIRED** for the ID Definition XML to be published *AND* be a valid UXP Identity. If no value is defined, then the publication process generates an error indicating this attribute has a problem.

3.3.3.2 ID-Level Rules

Rules are the defined attributes governing access to a UXP Object. Listed in the Rule blocks are the various access parameters and/or subsequent actions for violating any access parameter for a UXP Object. These Rules are *ONLY* editable in the ID Definition XML by the Identity owner/creator. Once the XML is published, these attributes are cloaked and inaccessible.

In the ID Definition XML, the Rules are structured by their title with their corresponding attributes listed below.

Many of the attributes within a single Rule block are stand-alone parameters that will execute once the field is appropriately populated. However, there are certain Rules with attributes that require other parameters and/or settings to be filled in a separate Rule block to fully activate the initial attribute. These Rule attribute relationships will be identified in their individual sections below.

Rule blocks can exist with empty attributes or contain no attributes and be successfully published to a UXP Identity.

There are two levels of Rule blocks: *Identity-Level* (ID) and *User-Level*. In the XML, the ID and User-Level Rules are defined by the Identity owner/creator.

ID-Level Rules: *ID-Level Rules* are global parameters that apply to all Users.

ID-Level Rule blocks are listed in the Rules section that begins after the public information in the ID Definition XML.

The ID-Level Rule blocks include the following:

- Access
- Restrictions
- Configurations
- Alerts
- Events

- Schedule

User-Level Rules: *User-Level Rules* are parameters that apply only to that individual User. These rules are defined, if needed, by the Identity owner/creator.

User-Level Rule blocks are listed separately from the ID-Level Rule blocks. These blocks are located in the *Users / Rules* section near the end of the ID Definition XML.

User-Level Rule blocks* include the following:

- User Configurations
- User Approvals
- User Schedule

***Note:** Configurations, Approvals, and Schedules at the ID-Level are structured identically as these listed at the User-Level. Having both Levels defined isn't required. However, in the event the same Rule block is defined at both ID and User-Levels, the more restrictive value is honored.

User-Level Privileges: Additionally, at the User-Level, there are UXP Object-related activity *Privileges* that are assigned to each User by the Identity owner/creator. *These Privileges are listed in the individual User's public information.*

These Privileges include the following:

- Read
- Write
- Delete
- Print
- Copy
- Sign
- ReadEvents
- Owner
- ReadSignature

3.3.3.2.1 Access

Access attributes control time and access limits for a UXP Object.

Figure 1. Access Rule Block in the ID Definition XML

```
<Rule name="Access">
    <AdvancedDataLogging type="bool"></AdvancedDataLogging>
    <Compliance type="int"></Compliance>
    <MaximumAccesses type="int"></MaximumAccesses>
    <MaximumCycleFailures type="int"></MaximumCycleFailures>
    <MaximumIdleTime type="int"></MaximumIdleTime>
    <MaximumTotalFailures type="int"></MaximumTotalFailures>
    <UseLocalTime type="bool"></UseLocalTime>
    <Workflow type="bool"></Workflow>

  </Rule>
```

Table 2. Access Attributes

Access Attribute	Datatype	Description
AdvancedDataLogging	Boolean	Detailed debugging information is captured and written to the external Sertainty log for the current application. **Default:** empty or false
Compliance	Number	This attribute is logically used to fulfill a simple compliance requirement. *It is not a matrix*. This specifically defines the self-destruct (expiration) date/time for the UXP Object. This value is entered as number representing the *total number of days* until the data in the UXP Object self-destructs. The result of the data self-destructing leaves an empty “invalid UXP Object” on disk. The start date/time is equal to the date when the UXP Object was created. **Example:** If a UXP Object was created Feb. 22, 2021 and need to self-destruct on Nov. 15, 2025, then the value entered for this attribute would be 1,727.

Access Attribute	Datatype	Description
		If the attribute is set to zero, no compliance date is active. **Default:** empty or zero **Note:** If a specified date/time is defined, then it is recommended to ALSO define the *UntrustedTimeDeny* attribute as true in the *Restrictions Rule* block. Having this attribute defined as true prevents a spoofing attempt to change the Compliance date/time for a UXP Object that could result in the data self-destructing prematurely or the date itself being extended. With this *UntrustedTimeDeny* attribute set as true, access to the Object would be simply denied.
MaximumAccesses	Number	This defines the maximum number of times the UXP Object can be successfully accessed before the Object's natural expiration date. This date is defined in the Compliance attribute in this Rule block. If the attribute is set to zero, access is unlimited. **Default:** empty or zero
MaximumCycleFailures	Number	This defines the maximum number of failed authentication cycles permitted *per authentication session*. If the maximum number is reached, then access to the UXP Object is denied without indicating a reason. A cycle is defined as a single set of Challenge Pairs presented during an authentication session. The required number of Pairs in a set is defined in the *EveryAuthenticationPrompt* attribute in the Restrictions Rule block. Failed Responses are not indicated during the authentication cycle. When a cycle fails, the next cycle is *not* a mathematical double of the previous cycle of presented Challenge Pairs. The number of Challenge Pairs added after a failed cycle is generated randomly based on a calculation of the number of incorrect Responses. **Example:** If this attribute is set to 5, a User can fail 4 consecutive authentication cycles and still successfully authenticate into the UXP Object in the 5th cycle. If the User

Access Attribute	Datatype	Description
		fails in the 5th cycle, access to the UXP Object is denied without indicating a reason. If the User successfully authenticates during any cycle *before* surpassing the maximum, the total failed cycle count resets to zero. If this attribute is set to zero, access is unlimited. **Default:** empty or zero
MaximumIdelTime	Number	This defines the maximum number of seconds that a UXP Object can remain idle. If idle time exceeds this value, the UXP Object will close without warning. If the attribute is set to zero, the Object will remain open until it is intentionally closed by a process or User. **Default:** empty or zero
MaximumTotalFailures	Number	This defines the maximum *total* number failed consecutive authentication cycles permitted to the UXP Object. The failed consecutive authentication cycle number is counted from *all authentication sessions.* The total number applies through the UXP Object's natural expiration date. This date is defined in the Compliance attribute in this Rule block. If the maximum total is reached, then contents of the UXP Object self-destruct. The result of the data self-destructing leaves an empty "invalid UXP Object" on disk. A cycle is defined as a single set of Challenge Pairs presented during an authentication session. The required number of Pairs in a set is defined in the *EveryAuthenticationPrompt* attribute in the Restrictions Rule block. Failed Responses are not indicated during the authentication cycle. When a cycle fails, the next cycle is *not* a mathematical double of the previous cycle of presented Challenge Pairs.

Access Attribute	Datatype	Description
		The number of Challenge Pairs added after a failed cycle is generated randomly based on a calculation of the number of incorrect Responses. **Example:** If this attribute is set to 12, a User can fail 11 consecutive cycles and still successfully authenticate into the UXP Object in the 12th consecutive cycle. The 11 failed cycles can span 1 or more authentication *sessions*. If the User fails in the 12th consecutive cycle, access to the UXP Object is denied without indicating a reason, AND the contents of the UXP Object self-destruct. If the User successfully authenticates within the 12 consecutive cycles before surpassing the maximum, the total failure count resets to zero. If this attribute is set to zero, access is unlimited. **Default:** empty or zero
UseLocalTime	Boolean	The UXP Object considers local machine date and time to be trusted. If disabled, the date and time will only be trusted if acquired from a trusted timer server. Currently, UXP Technology maintains a trusted time and location server to establish trusted time. **Default:** empty
Workflow	Boolean	When this is set to *true*, this is an indicator to the UXP System that the UXP Object will not permit interactive authentication. This indicator applies to machine automated workflows. For this attribute to execute, it has a dependency on having a corresponding Auto-Unprotect script uniquely tied to the Workflow Identity. This script must be created at the same time as the Machine Workflow Identity is being created.

Access Attribute	Datatype	Description
		Basically, the Workflow Challenge Pairs are auto-generated ONLY once and aren't visible in the Workflow Identity creation process. Therefore, the only time to capture these Challenge Pairs for them to be included in the Auto-Unprotect script is during the Workflow Identity creation. See Data Protector API Guide for more information. **Default:** empty or false

3.3.3.2.2 Restrictions

Restrictions are the assigned actions that take place when a specific Rule violation occurs during authentication. These resulting actions are one or more of the following:

- Send an Approval
- Deny access
- Destroy data – the contents of the UXP Object self-destruct leaving an empty "invalid Object" on disk
- Present additional Prompts (Challenge Pairs)

A specific Rule violation and its assigned Restriction are dependent upon that specific Rule being configured and enabled. These dependencies are indicated in their respective tables below.

> **Note**: Most of the attributes listed in Restrictions do have a dependency on another Rule, but there are some attributes that don't have a dependency. The dependencies are identified within the sections below.

The Restriction attributes within the block are based on the Rule and the type of violation within that Rule.

Figure 2. Restrictions Rule Block in the ID Definition XML

```
<Rule name="Restrictions">
    <ConfigurationApproval type="bool"></ConfigurationApproval>
    <ConfigurationDeny type="bool"></ConfigurationDeny>
    <ConfigurationDestroy type="bool"></ConfigurationDestroy>
    <ConfigurationPrompts type="int"></ConfigurationPrompts>
    <EveryAuthenticationApproval type="bool"></EveryAuthenticationApproval>
    <EveryAuthenticationPrompts type="int"></EveryAuthenticationPrompts>
```

```
    <HardwareApproval type="bool"></HardwareApproval>
    <HardwareDeny type="bool"></HardwareDeny>
    <HardwareDestroy type="bool"></HardwareDestroy>
    <HardwarePrompts type="int"></HardwarePrompts>
    <LocationApproval type="bool"></LocationApproval>
    <LocationDeny type="bool"></LocationDeny>
    <LocationDestroy type="bool"></LocationDestroy>
    <LocationPrompts type="int"></LocationPrompts>
    <MovementApproval type="bool"></MovementApproval>
    <MovementDeny type="bool"></MovementDeny>
    <MovementDestroy type="bool"></MovementDestroy>
    <MovementPrompts type="int"></MovementPrompts>
    <NetworkApproval type="bool"></NetworkApproval>
    <NetworkDeny type="bool"></NetworkDeny>
    <NetworkDestroy type="bool"></NetworkDestroy>
    <NetworkPrompts type="int"></NetworkPrompts>
    <Preset type="string"></Preset>
    <ScheduleApproval type="bool"></ScheduleApproval>
    <ScheduleDeny type="bool"></ScheduleDeny>
    <ScheduleDestroy type="bool"></ScheduleDestroy>
    <SchedulePrompts type="int"></SchedulePrompts>
    <UntrustedSystemApproval type="bool"></UntrustedSystemApproval>
    <UntrustedSystemDeny type="bool"></UntrustedSystemDeny>
    <UntrustedSystemDestroy type="bool"></UntrustedSystemDestroy>
    <UntrustedSystemPrompts type="int"></UntrustedSystemPrompts>
    <UntrustedTimeApproval type="bool"></UntrustedTimeApproval>
    <UntrustedTimeDeny type="bool"></UntrustedTimeDeny>
    <UntrustedTimeDestroy type="bool"></UntrustedTimeDestroy>
    <UntrustedTimePrompts type="int"></UntrustedTimePrompts>
</Rule>
```

3.3.3.2.2.1 Configuration Restrictions

A Configuration in UXP Technology context is composed of three types of information: *hardware, location*, and *network*. Together, this combination provides a unique fingerprint to specify exactly where a UXP Object can be accessed.

At least one known Configuration is required to be included in the Configurations Rule block for any Configuration Restriction to execute. Configuration attributes are included in the Configurations Rule block*.

> ***Note:** The necessary Configuration attributes are created separately using the UXP Configuration function in the respective APIs. This function is an automated process that collects all attributes for hardware, location, and network. These attributes are presented in a separate XML document. From this XML, the desired attributes can be included in the Configurations Rule block within the Identity Definition XML.

As stated, a known Configuration is required for any Configuration Restriction to execute, but an unknown Configuration can be added if the following conditions are true:

- A UXP Object is “read/write architecture”
- A successful User authentication to that UXP Object

The result of these conditions is the previously unknown Configuration is now a known Configuration for that UXP Object. In future authentication attempts of this UXP Object, this Configuration will be recognized.

The ability to override an unrecognized Configuration Restriction applies to the following attributes:

- ConfigurationApproval
- ConfigurationPrompts

If the UXP Object is “read-only architecture”, the Configuration Restriction will always execute for unknown Configurations.

A Configuration Restriction can be defined at the global ID and/or User-Levels.

Table 3. Configuration Restriction Attributes

Configuration Restriction Attribute	Datatype	Description
ConfigurationApproval	Boolean	If the current Configuration is unrecognized, an Approval is required to continue with authentication into the UXP Object.

Configuration Restriction Attribute	Datatype	Description
		An Approval is defined in the Approvals and/or User Rule block – ID and/or User-Level(s). **Default:** empty or false
ConfigurationDeny	Boolean	If the current Configuration is unrecognized, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
ConfigurationDestroy	Boolean	If the current Configuration is unrecognized, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
ConfigurationPrompts	Number	If the current Configuration is unrecognized, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.2 Every Authentication Restrictions

Every Authentication Restrictions are clear in their purpose. At every authentication attempt into a UXP Object, either an Approval and/or a specific number of Challenge Pairs are required.

Table 4. Every Authentication Restriction Attributes

Every Authentication Restriction Attribute	Datatype	Description
EveryAuthenticationApproval	Boolean	An Approval is required for every authentication attempt into the UXP Object.

Every Authentication Restriction Attribute	Datatype	Description
		An Approval is defined in the Approvals Rule block – ID or User-Level(s). **Default:** empty or false
EveryAuthenticationPrompts	Number	This designates the specific number of Challenge Pairs *required* for every authentication attempt into the UXP Object. **Default:** 1

3.3.3.2.2.3 Hardware Restrictions

Hardware Restrictions focus on the device(s) where a UXP Object is accessed. As discussed in Configuration Restrictions, hardware is one of the three types of information within a Configuration. If network and location aren't of interest, then a specific Hardware-only Configuration can be defined.

Just like the Configuration containing hardware, location, and network, a Hardware Configuration provides a unique fingerprint of the device to specify where a UXP Object can be accessed.

At least one known Hardware Configuration is required to be included in the Configuration Rule block for any Hardware Restriction to execute. Hardware Configurations are included in the Configurations Rule block*.

> ***Note:** The necessary Configuration attributes are created separately using the UXP Configuration functions in the respective APIs. This function is an automated process that collects *all* attributes for hardware, location, and network. These attributes are presented in a separate XML document. From this XML, the desired attributes for hardware can be transcribed into the Configurations Rule block within the Identity Definition XML.

As stated, a known Hardware Configuration is required for any Hardware Restriction to execute, but an unknown Hardware Configuration can be added if the following conditions are true:

- A UXP Object is "read/write architecture"
- A successful User authentication to that UXP Object

The result of these conditions is the previously unknown Hardware Configuration is now a known Hardware Configuration for that UXP Object. In future authentication attempts of this UXP Object, this Hardware Configuration will be recognized.

The ability override for an unrecognized Hardware Restriction applies to the following attributes:

- HardwareApproval

- HardwarePrompts

If the UXP Object is “read-only architecture”, the Hardware Restriction will always execute for unknown Hardware Configurations.

A Hardware Restriction can be defined at the global ID and/or User-Levels.

Table 5. Hardware Restriction Attributes

Hardware Restriction Attribute	Datatype	Description
HardwareApproval	Boolean	If the current Hardware Configuration is unrecognized, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false
HardwareDeny	Boolean	If the current Hardware Configuration is unrecognized, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
HardwareDestroy	Boolean	If the current Hardware Configuration is unrecognized, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
HardwarePrompts	Number	If the current Hardware Configuration is unrecognized, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.4 Location Restrictions

Location Restrictions focus on the geographical location where a UXP Object is accessed. As discussed in Configuration Restrictions, location is one of the three types of information within a Configuration. If network and hardware aren't of interest, then a specific Location-only Configuration can be defined.

Just like the Configuration containing network and hardware, a Location Configuration provides a unique fingerprint of the geographical location to specify where a UXP Object can be accessed.

At least one known Location Configuration is required to be included in the Configuration Rule block for any Location Restriction to execute. Location Configuration(s) are included in the Configurations Rule block*.

> ***Note:** The Location Configuration attributes are created separately using the UXP Configuration functions in the respective APIs. This function is an automated process that collects *all* attributes for hardware, location, and network. These attributes are presented in a separate XML document. From this XML, the desired location attributes can be transcribed into the Configurations Rule block within the Identity Definition XML.

As stated, a known Location Configuration is required for any Location Restriction to execute, but an unknown Location Configuration can be added if the following conditions are true:

- A UXP Object is "read/write architecture"
- A successful User authentication to that UXP Object

The result of these conditions is the previously unknown Location Configuration is now a known Location Configuration for that UXP Object. In future authentication attempts of this UXP Object, this Location Configuration will be recognized.

The ability to override for an unrecognized Location Restriction applies to the following attributes:

- LocationApproval
- LocationPrompts

If the UXP Object is "read-only architecture", the Location Restriction will always execute for unknown Location Configurations.

A Location Restriction can be defined at the global ID and/or User-Levels.

Table 6. Location Restriction Attributes

Location Restriction Attribute	Datatype	Description
LocationApproval	Boolean	If the current Location is unrecognized, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false
LocationDeny	Boolean	If the current Location Configuration is unrecognized, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
LocationDestroy	Boolean	If the current Location Configuration is unrecognized, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
LocationPrompts	Number	If the current Location Configuration is unrecognized, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.5 Movement Restrictions

Movement Restrictions control the *file-path-location* on a device or server where a UXP Object is permitted access.

The default *file-path-location* is where the UXP Object was generated, but this default path doesn’t populate the attribute.

The optional attribute to define an alternative access *file-path-location(s)* is added to the Configurations Rule block.*

*__Note:__ A Configuration in the block is required before a *file-path-location* can be defined.

This optional *file-path-location* attribute can be utilized both at ID and/or User-Levels.

Figure 3. ID-Level File Path Attribute Placement in the Configurations Rule Block

```
<Rule name="Configurations">
    <Configurations>
     <Configuration>
      <Id type="int">1186353359</Id>
      <Name type="string">Nashville-TN-N-108.70.121.20</Name>
      <Enabled type="bool">true</Enabled>
      <!---->
      <Device>
       <Id type="int">2499348916</Id>
       <Name type="string">Macbook-MBP-2</Name>
       <FilePath>/*</FilePath>
       <Architecture type="string">x86_64</Architecture>
```

Figure 4. User-Level File Path Attribute Placement in the UserConfigurations Rule Block

```
<Rules>
     <Rule name="UserConfigurations">
      <Configurations />
       <Configuration>
      <Id type="int">1186350959</Id>
      <Name type="string">Nashville-TN-N-106.70.121.20</Name>
      <Enabled type="bool">true</Enabled>
      <!---->
      <Device>
       <Id type="int">24993407916</Id>
       <Name type="string">Test2-MBP-2</Name>
       <FilePath>/*</FilePath>
```

```
    <Architecture type="string">x86_64</Architecture>
  </Rule>
```

Table 8. Movement Restriction Attributes

Movement Restriction Attribute	Datatype	Description
MovementApproval	Boolean	If the current file-path-location is unrecognized, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false
MovementDeny	Boolean	If the current file-path-location is unrecognized, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
MovementDestroy	Boolean	If the current file-path-location is unrecognized, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
MovementPrompts	Number	If the current file-path-location is unrecognized, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.6 Network Restrictions

Network Restrictions focus on the geographical location where a UXP Object is accessed. As discussed in Configuration Restrictions, location is one of the three types of information within a Configuration. If location and hardware aren’t of interest, then a specific Network-only Configuration can be defined.

Just like the Configuration containing location and hardware, a Network Configuration provides a unique fingerprint of the geographical location to specify where a UXP Object can be accessed.

At least one known Network Configuration is required to be included in the Configuration Rule block for any Network Restriction to execute. Network Configuration(s) are included in the Configurations Rule block*.

> ***Note:** The Network Configuration attributes are created separately using the UXP Configuration functions in the respective APIs. This function is an automated process that collects *all* attributes for hardware, location, and network. These attributes are presented in a separate XML document. From this XML, the desired network attributes can be transcribed into the Configurations Rule block within the Identity Definition XML.

As stated, a known Network Configuration is required for any Network Restriction to execute, but an unknown Network Configuration can be added if the following conditions are true:

- A UXP Object is “read/write architecture”
- A successful User authentication to that UXP Object

The result of these conditions is the previously unknown Network Configuration is now a known Network Configuration for that UXP Object. In future authentication attempts of this UXP Object, this Network Configuration will be recognized.

The ability to override for an unrecognized Network Restriction applies to the following attributes:

- Network Approval
- Network Prompts

If the UXP Object is “read-only architecture”, the Network Restriction will always execute for unknown Network Configurations.

A Network Restriction can be defined at the global ID and/or User-Levels.

Table 9. Network Restriction Attributes

Network Restriction Attribute	Datatype	Description
NetworkApproval	Boolean	If the current Network is unrecognized, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false

Network Restriction Attribute	Datatype	Description
NetworkDeny	Boolean	If the current Network Configuration is unrecognized, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
NetworkDestroy	Boolean	If the current Network Configuration is unrecognized, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
NetworkPrompts	Number	If the current Network Configuration is unrecognized, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.7 Preset

This value is the *name* of a RulePreset XML defined prior to generating the ID Definition XML. This Rule Preset XML is imported into the ID Definition XML. Sertainty recommends using a descriptive name coinciding with the actions defined in the Rule blocks.

> **Example:** *Confidential* is the name for a Rule Preset XML controlling the organization’s access to its highly classified data.

The Preset attribute is an *informational reference* for the specific Rule Preset XML included in the ID Definition XML. This attribute has no impact on the UXP Object construction.

Table 10. Preset Attribute

Preset Attribute	Datatype	Description
Preset	String	Name of the pre-defined Rule Preset XML that populates the ID Definition XML template.

3.3.3.2.2.8 Schedules Restrictions

Schedule Restrictions are the resulting UXP Object actions if a User violates a defined Schedule. For a Schedule Restriction(s) to execute, an active Schedule MUST be defined in the Schedule and/or User Schedule Rule block. A Schedule is a specific time-window when a UXP Object can be accessed.

A Schedule Restriction can be defined for a global ID and/or User-Level Schedule.

Table 11. Schedule Restriction Attributes

Schedule Restriction Attribute	Datatype	Description
ScheduleApproval	Boolean	If the active Schedule is violated, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals and/or User Rule block – ID and/or User-Level(s). **Default:** empty or false
ScheduleDeny	Boolean	If the active Schedule is violated, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
ScheduleDestroy	Boolean	If the active Schedule is violated, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
SchedulePrompts	Number	If the active Schedule is violated, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.9 Untrusted System Restrictions

An Untrusted System corresponds to a virtual machine that potentially is masked or hidden. The UXP Technology system scans for these details. This is a separate function external to the Configurations Rule block.

Table 12. Untrusted System Restriction Attributes

Untrusted System Restriction Attribute	Datatype	Description
UntrustedSystemApproval	Boolean	If the current operating system is an untrusted virtual machine, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false
UntrustedSystemDeny	Boolean	If the current operating system is an untrusted virtual machine, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
UntrustedSystemDestroy	Boolean	If the active Schedule is violated, the contents of UXP Object self-destruct. The result of this action leaves an empty “invalid UXP Object” on disk. **Default:** empty or false
UntrustedSystemPrompts	Number	If the current operating system is an untrusted virtual machine, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.2.10 Untrusted Time Restrictions

Untrusted Time corresponds with the UXP Technology system process that validates date and time utilizing an external server. If a UXP Object is unable to reach the internet to validate date and time, then the Object is flagged with untrusted time.

Table 13. Untrusted Time Restriction Attributes

Untrusted Time Restriction Attribute	Datatype	Description
UntrustedTimeApproval	Boolean	If the current date and time can't be verified, an Approval is required to continue with authentication into the UXP Object. An Approval is defined in the Approvals Rule block – ID and/or User-Level(s). **Default:** empty or false
UntrustedTimeDeny	Boolean	If the current date and time can't be verified, access to the UXP Object is denied without indicating a reason. **Default:** empty or false
UntrustedTimeDestroy	Boolean	If the current date and time can't be verified, the contents of UXP Object self-destruct. The result of this action leaves an empty "invalid UXP Object" on disk. **Default:** empty or false
UntrustedTimePrompts	Number	If the current date and time can't be verified, a specified number of Challenge Pairs are added during authentication. **Default:** empty or zero

3.3.3.2.3 Configurations

A Configuration in UXP Technology context is composed of three types of information: *hardware, location, and network*. Together, this combination provides a unique *fingerprint* to specify exactly where a UXP Object can be accessed.

The necessary Configuration attributes are created separately using the UXP Configuration function in the respective APIs. This function is an automated process that collects *all attributes* for hardware, location, and network. These attributes are presented in a separate XML document that structurally matches the structure of the ID Definition XML. From this XML, the desired attributes can be included in the Configurations Rule block with the Identity Definition XML.

One or more Configurations can be defined at the global ID and/or User-Levels. (See Appendix A – section 4.2 for an example.)

Figure 5. Configurations Rule Block in the ID Definition XML

```
<Rule name="Configurations">
  <Configurations>
  <Configuration>
   <Id type="int"></Id>
   <Name type="string"></Name>
   <Enabled type="bool"></Enabled>
   <!---->
   <Device>
    <Id type="int"></Id>
    <Name type="string"></Name>
    <Architecture type="string"></Architecture>
    <CpuModel type="string"></CpuModel>
    <CpuSN type="string"></CpuSN>
    <CpuVendor type="string"></CpuVendor>
    <DeviceType type="string"></DeviceType>
    <MachineModel type="string"></MachineModel>
    <MachineName type="string"></MachineName>
    <MachineSN type="string"></MachineSN>
    <MachineUUID type="string"></MachineUUID>
    <MachineVendor type="string"></MachineVendor>
```

```
  <OsFileId type="string"></OsFileId>
  <OsMachine type="string"></OsMachine>
  <OsName type="string"></OsName>
  <OsType type="string"></OsType>
  <OsUserName type="string"></OsUserName>
  <OsVersion type="string"></OsVersion>
  <Ram type="string"></Ram>
  <TimeZone type="string"></TimeZone>
  <TotalMemory type="string"></TotalMemory>
  <Vendor type="string"></Vendor>
</Device>
<!---->
<Location>
  <Id type="int"></Id>
  <Name type="string"></Name>
  <Address type="string"></Address>
  <City type="string"></City>
  <Country type="string"></Country>
  <InvalidLatitude type="string"></InvalidLatitude>
  <InvalidLongitude type="string"></InvalidLongitude>
  <InvalidRange type="string"></InvalidRange>
  <Latitude type="string"></Latitude>
  <Longitude type="string"></Longitude>
  <Range type="string"></Range>
  <State type="string"></State>
  <Timestamp type="string"></Timestamp>
  <Zipcode type="string"></Zipcode>
</Location>
<!---->
<Network>
  <Id type="int"></Id>
  <Name type="string"></Name>
```

```
        <InvalidIp type="string"></InvalidIp>
        <IpAddress type="string"></IpAddress>
      </Network>
    </Configuration>
  </Configurations>
```

3.3.3.2.4 Alerts

Alert attributes trigger messages to be sent from the UXP Object when an access attempt fails. The message content along with where the message is sent is defined in the Alerts Rule block.

Figure 6. Alerts Rule Block in the ID Definition XML

```
<Rule name="Alerts">
    <EmailAddress type="string"></EmailAddress>
    <IncludeDevice type="bool"></IncludeDevice>
    <IncludeLicense type="bool"></IncludeLicense>
    <IncludeLocation type="bool"></IncludeLocation>
    <SMSAddress type="string"></SMSAddress>
    <UseEmail type="bool"></UseEmail>
    <UseSMS type="bool"></UseSMS>

  </Rule>
```

Table 14. Alerts Attributes

Alerts Attribute	Datatype	Description
EmailAddress	String	This is the specified *email address* where the Alert message is sent. The following example User information is shown in the email:

Alerts Attribute	Datatype	Description
		On 3/4/21, 3:14pm, "Sertainty" < sertainty.messenger@sertainty.com> wrote: UXP Object access denied at this time. Please try again later. 2021-03-04T15:14:49 Sertainty UXP Object title: Description: \UXP Owner: TechEd1 User: TechEd1 (TechEdUser1) Created:2021-03-04T15:14:28 File accessed: /Users/Test1/Documents/!-all-learning/WorkingDirectory/test-alerts.uxp **Sender address:** sertainty.messenger@sertainty.com **Default:** empty
IncludeDevice	Boolean	The message content includes the hardware attributes where the failed access attempt occurred for the UXP Object. These attributes are a similar collection that would be gathered for a Configuration. This collection occurs in real time and is facilitated by UXP Technology. The following example shows the hardware attributes collected and sent via email: Device signature: 1665445208 Architecture: x86_64 CpuModel: Intel(R) Core(TM) i9-6950HK CPU @ 2.90GHz CpuSN: CpuVendor: GenuineIntel DeviceId: 1665907208 DeviceName: Test-Test-MBP-2 DeviceType: Mobile Device MachineModel: MacBookPro15,1 MachineName: Test-MBP-2 MachineSN: C02XT086JGH7 MachineUUID: 565E4C46-9652-5759-BBCA-47A6561C3CA7 MachineVendor: Apple OsFileId: 32cf5e338830d OsMachine: x86_64 OsName: MacOSX OsType: Mac OS X OsUserName: msw OsVersion: 10.15.7 Ram: 16384 TimeZone: -360 TotalMemory: 17179869184 Vendor: Apple **Default:** empty or false
IncludeLicense	Boolean	The message content includes the Sertainty License information for the User or Machine

Alerts Attribute	Datatype	Description
		Instance that failed an access attempt for the UXP Object. The following example shows the License information collected and sent via email: License: Activated: 1 ActivationEnd: 2021-01-22T16:16:16 ActivationStart: 2020-12-23T16:16:16 DefaultPrivileges: 32767 DemoMode: 0 Description: Internal Sertainty DisableOnExpired: 0 Expiration: 2021-04-19T12:55:49 ExpirationDays: 90 Granted: AltRealities,Alter,AssignLicense,Copy,Create,License,Print,Read,Read Audit,ReadSignature,Sign,SuperUser,Unlimited,Write Key: 0000-0000-0000-001F LastExecution: None LicenseType: Sertainty Name: Melani Smith Weed (SU) NotifySertainty: 1 Product: UXP SmartID: 1 SmartMessage: 1 UserGroup1: Sertainty Developer Version: 4 applicationAdmin: 1 applicationGroupEnabled: 0 applicationID: Xv745Hsuuues44$$38mmMjqw200Mnj89 applicationProtectedOnly: 0 canEditRules: 1 canUseAgentTasks: 1 canUseDelegates: 1 canUseDomains: 1 canUseExperimental: 1 canUseIdLibrary: 1 canUseSDK: 1 canUseSQL: 1 canUseScriptEngine: 1 canUseVFS: 1 cardMax: 99 userMax: 99 Owner.Name: License Manager Owner.Company: Sertainty Corporation Owner.City: Nashville Owner.State: TN Owner.Zipcode: 37217 Owner.Country: USA Owner.Phone: 6158465500 Owner.Email: license.manager@sertainty.com **Default:** empty or false
IncludeLocation	Boolean	The message content includes the location attributes where the failed access attempt occurred for the UXP Object. These attributes are a similar collection that would be gathered in a

Alerts Attribute	Datatype	Description
		Configuration. This collection occurs in real time and is facilitated by UXP Technology. The following example shows the location attributes collected and sent via email: Location signature: 3878159696 Address: 930 River Road City: Franklin Country: US InvalidIp: InvalidLatitude: 0.000 InvalidLongitude: 0.000 InvalidRange: 0.000 IpAddress: 108.23.121.20 Latitude: 35.908 LocationId: 3878159696 LocationName: Franklin-TN Longitude: -86.234 NetworkId: 3476494946 NetworkName: N-108.34.121.20 Range:0.000 ScoreAddress: ScoreCity: ScoreCountry: ScoreIP: ScoreState: ScoreZipcode: State: TN Timestamp: 1614891837631 (2021-03-04T15:03:57) Zipcode: 37234 **Default:** empty or false
SMSAddress	String	This is the specified *SMS address* where the Alert message is sent. The content set provided using this delivery method is a condensed list of the hardware and/or location attributes. The information is sent in multiple text messages. The following example shows the location and hardware attributes collected and sent via text message:

Alerts Attribute	Datatype	Description
		UXP Alert: UXP Object access denied at this time. Please try again. UXP title: NoName User: TechED1 Addr: 930 Del Rio Pike, Franklin, TN 37064 IP:108.70.1221.20 Lat: 34.931 Lng: -86.879 SN: C02XTO26T GH7 OS: MacOSX User: Test1 The License information, if enabled, is excluded in SMS due to parsing capabilities of this information. The SMSAddress utilizes the preferred mobile service provider's email address used to deliver SMS messages. **Example:** 5551234567@messaging.sprintpcs.com **Default:** empty
UseEmail	Boolean	This is a preference attribute for the Alert message is received. The **EmailAddress** attribute in the Alerts Rule block must be populated with an email address. **Default:** empty or false
UseSMS	Boolean	This is a preference attribute for the Alert message is received. The **SMSAddress** attribute in the Alerts Rule block must be populated with an SMS address. **Default:** empty or false

3.3.3.2.5 Approvals

The Approvals Rule block is directly associated to human authentication using an external multi-factor authentication (MFA) client. UXP Technology has selected DUO as its current external MFA client. DUO is

coded into UXP Technology. This web-based application requires an account with a user to be set up by the customer.

Once the account is set up, specific DUO account details are utilized in configuring an Approval in this block.

DUO offers a free version along with price-friendly upgraded version. To set up a DUO account, go to https://duo.com/

Figure 7. Approvals Rule Block in ID Definition XML

```
<Rule name="Approvals">
    <ExternalLength type="int"></ExternalLength>
    <Approval name="">
      <Enabled type="bool"></Enabled>
      <Address type="string"></Address>
      <Description type="string"></Description>
      <Prompt type="string"></Prompt>
      <Type type="string"></Type>
      <Response type="string"></Response>
    </Approval>

  </Rule>
```

Table 15. Approval Attributes in ID Definition XML

Approval Attribute	Datatype	Description
ExternalLength	Number	This attribute is required for legacy UXP Technology versions 3.4 or lower and is unrelated to the current Approvals process using DUO. This specifies the number of randomly-generated characters for the Approval code. This code would be utilized for an email Approvals process.* ***Note:** In the event that a UXP Object is being authenticated on a legacy version of UXP Technology prior to DUO integration, the Approval process reverts to sending an Approval code to a specified email address.

Approval Attribute	Datatype	Description
		This email address is required in the **Address** attribute in this block. **Default:** 6, if Approval Rule block is enabled
Approval Name	String	This is a unique identifying title or name for the Approval. This attribute doesn't affect the Approval function using DUO in UXP Technology. If a name is not defined, then the UXP System defaults to the information in Prompt attribute in this block. **Default:** empty
Enabled	Boolean	This enables the MFA Approval process. **Default:** empty or false
Address	String	This is an email address. If the UXP Object is authenticating on a legacy version of UXP Technology (3.4 or lower) prior to DUO integration, the Object will send the Approval code to this email address as an alternative to using DUO.* ***Note:** The **ExternalLength** attribute in this block must contain a number for the Address attribute to be used as an alternative. **Default:** empty
Description	String	This is the content included with the DUO Approval message.* ***Note:** It is recommended to use very specific descriptive information for easy identification of the requestee of the Approval. **Default:** empty
Prompt	String	This is the specific Prompt connected to this Approval and is included with the DUO Approval request.* The Prompt is **required** for using DUO for UXP Object authentication.

Approval Attribute	Datatype	Description
		***Note:** It is recommended to make the Prompt very specific for easy identification of the requestee of the Approval. **Default:** empty
Type	String	This defines the method of the Approval configuration and the delivery mechanism. **Required** **Type:** MFA
Response	String	The specific DUO User information is used in this string attribute. Response is a **required** attribute. The DUO account components used in the Response attribute are the following: • **Username** – This is set up in the DUO account. • **Integration key** – This is auto-generated by DUO for the user account. • **Secret key** – This is auto-generated by DUO for the user account. • **API hostname** – This is the URL that tells the UXP System how to communicate with DUO. • **Timeout** – This is a value in *seconds* indicating how long the UXP System will wait for DUO to respond to the Approval request sent to DUO by the UXP Object. If the time passes before DUO responds, the UXP Object denies access without indicating a reason. **Default:** 30 seconds These components are placed in a specific order in the Response attribute and are shown below. **Response String:** DUO:Username:IntegrationKey:SecretKey:APIhostname:Timeout

Approval Attribute	Datatype	Description
		See Appendix A – section 4.3 for an example.

3.3.3.2.6 Events

Events control how the external UXP Engine records UXP Object activities. Various Event actions can be defined to trigger an entry to be recorded into an *internal UXP Object Event Log* or an *external Event Log entry located in UXP Event Service*. See UXP Services Guide.

An Event Log entry represents a single UXP Object activity.

Event activity information collected is a combination of UXP Object details. Included are Username, Object name, Object title and description (if available), and full configuration details on where the Object Event activity occurred.

Figure 8. Events Rule Block in ID Definition XML

```
<Rule name="Events">
    <EmailAddress type="string"></EmailAddress>
    <ExternalKey type="string"></ExternalKey>
    <FileSpec type="string"></FileSpec>
    <LogAccesses type="bool"></LogAccesses>
    <LogCustom type="bool"></LogCustom>
    <LogFailures type="bool"></LogFailures>
    <LogMessages type="bool"></LogMessages>
    <LogRepeats type="bool"></LogRepeats>
    <RecordEmail type="bool"></RecordEmail>
    <RecordExternal type="bool"></RecordExternal>
    <RecordFile type="bool"></RecordFile>
    <RecordLocal type="bool"></RecordLocal>
    <RecordRemote type="bool"></RecordRemote>
    <RecordSMS type="bool"></RecordSMS>
    <RemoteURL type="string"></RemoteURL>
    <SMSAddress type="string"></SMSAddress>

  </Rule>
```

Table 16. Events Attributes in ID Definition XML

Event Attribute	Datatype	Description
EmailAddress	String	This is an email address to deliver recorded UXP Object Event Log activities. **Optional** **Default:** empty
ExternalKey	String	This is a private key. When recording Events to an external callback routine, a private key must be provided to the API. The external routine must use this key to decode the Event Log data. **Optional** **Default:** empty
FileSpec	String	This is a specified file name and location for recording all Event activities for a UXP Object. The Event activities that are enabled are recorded. These activities are defined in the Event Rule block. **Optional** **Default:** empty
LogAccesses	Boolean	This creates an Event Log entry when a UXP Object has been accessed. **Default:** empty or false
LogFailures	Boolean	This creates an Event Log entry when an unsuccessful authentication attempt to the UXP Object occurs. **Default:** empty or false

Event Attribute	Datatype	Description
LogMessages	Boolean	This creates an Event Log entry when any external messages are sent from the UXP Object. **Example:** An Alert requiring location details for an unsuccessful authentication attempt is defined. When a failed access occurs to a UXP Object, an Alert with these location details is sent via email. An Event Log entry is also recorded. **Default:** empty or false
LogRepeats	Boolean	This creates an Event Log entry when repeated unsuccessful authentication attempts to a UXP Object have occurred. This is a particular indicator that some unauthorized person or process is trying to gain access to the Object beyond a single failed attempt. **Default:** empty or false
RecordEmail	Boolean	This sends the Event Log entry to the specified email defined in the **EmailAddress** attribute in the Events Rule block. **Default:** empty or false
RecordExternal	Boolean	This sends the Event Log entry to an external callback routine. **Default:** empty or false
RecordFile	Boolean	This records an Event Log entry in the file and locations specified in the **FileSpec** attribute in the Events Rule block. **Default:** empty or false
RecordLocal	Boolean	This records Event Log entries within the UXP Object.

Event Attribute	Datatype	Description
		Read-write architecture is **REQUIRED** for the UXP Object. **Default:** empty or false
RecordRemote	Boolean	This sends Event Log entries to a reachable UXP Services server. See UXP Services Guide. **Default:** empty or false
RecordSMS	Boolean	This sends the Event Log entry to the specified SMS address defined in the **SMSAddress** attribute in the Events Rule block. **Default:** empty or false
RecordURL	String	This is the UXP Services server URL. See UXP Services Guide. **Default:** empty
SMSAddress	String	This is the specified *SMS address* where the Event Log entry is sent. The content set provided using this delivery method is a condensed list of the defined Event attributes and other information. The information is sent in multiple text messages. The SMSAddress utilizes the preferred mobile service provider's email address used to deliver SMS messages. **Example:** 5551234567@messaging.sprintpcs.com **Default:** empty

3.3.3.2.7 Schedule

Schedule attributes define a day of the week and/or specific time-window when access is permitted to a UXP Object. When a Schedule is set up, the time-window and/or day is the ONLY time that a UXP Object can be accessed.

For a time-window Schedule, *a Start and End attribute must be defined*. If either a Start or End attribute is defined without an opposing attribute defined to create a time-window, UXP Technology recognizes the missing attribute. The Technology responds by populating the missing attribute with the current date and/or time.*

***Note:** This scenario may cause a date/time mis-match. The mis-match results in an invalid ID Definition XML, and publication will be prevented.

Start /End Attributes: All attributes require population in both the Start and End category. If only one attribute is populated, then UXP Technology will automatically fill in the empty attributes with the current date/time information. This may cause a date/time mis-match as noted above and create problems with publications.

Post Schedule Setup Requirements: Once a Schedule is set up, a Schedule Restriction in the Restrictions Rule block **MUST** be enabled in order for the Schedule to be fully active. The Schedule Restriction is the resulting UXP Object action if the Schedule is violated. Without an enabled Schedule Restriction, the Schedule will be ignored.

A Schedule can be defined at the global ID and/or User-Levels.

Figure 9. Schedule Rule Block in the ID Definition XML

```
<Rule name="Schedule">

    <Enabled type="bool"></Enabled>
    <DaySunday type="bool"></DaySunday>
    <DayMonday type="bool"></DayMonday>
    <DayTuesday type="bool"></DayTuesday>
    <DayWednesday type="bool"></DayWednesday>
    <DayThursday type="bool"></DayThursday>
    <DayFriday type="bool"></DayFriday>
    <DaySaturday type="bool"></DaySaturday>
    <StartDay type="int"></StartDay>
    <StartHour type="int"></StartHour>
    <StartMinute type="int"></StartMinute>
    <StartMonth type="int"></StartMonth>
    <StartYear type="int"></StartYear>
    <EndDay type="int"></EndDay>
    <EndHour type="int"></EndHour>
    <EndMinute type="int"></EndMinute>
```

```
    <EndMonth type="int"></EndMonth>
    <EndYear type="int"></EndYear>
</Rule>
```

Table 17. Schedule Attributes in the ID Definition XML

Schedule Attribute	Datatype	Description
Enabled	Boolean	This is enables the defined Schedule. **Default:** empty
DaySunday	Boolean	**True:** UXP Object access on Sunday is permitted.
DayMonday	Boolean	**True:** UXP Object access on Monday is permitted.
DayTuesday	Boolean	**True:** UXP Object access on Tuesday is permitted.
DayWednesday	Boolean	**True:** UXP Object access on Wednesday is permitted.
DayThursday	Boolean	**True:** UXP Object access on Thursday is permitted.
DayFriday	Boolean	**True:** UXP Object access on Friday is permitted.
DaySaturday	Boolean	**True:** UXP Object access on Saturday is permitted.
StartDay	Number	This specifies the day of the month on which **UXP Object** access starts. **Default:** -1 indicates any day
StartHour	Number	This specifies the hour of the day on which **UXP Object** access starts. **Default:** -1 indicates any hour

Schedule Attribute	Datatype	Description
StartMinute	Number	This specifies the minute of the hour on which **UXP Object** access starts. **Default:** -1 indicates any minute
StartMonth	Number	This specifies the month of the year on which **UXP Object** access starts. **Default:** -1 indicates any month
StartYear	Number	This specifies the year on which **UXP Object** access starts. **Default:** -1 indicates any year
EndDay	Number	This specifies the day of the month on which **UXP Object** access ends. **Default:** -1 indicates any day
EndHour	Number	This specifies the hour of the day on which **UXP Object** access ends. **Default:** -1 indicates any hour
EndMinute	Number	This specifies the minute of the hour on which **UXP Object** access ends. **Default:** -1 indicates any minute
EndMonth	Number	This specifies the month of the year on which **UXP Object** access ends. **Default:** -1 indicates any month
EndYear	Number	This specifies the year on which **UXP Object** access ends.

Schedule Attribute	Datatype	Description
		Default: -1 indicates any year

3.3.3.3 Users

Users is the third section of the ID Definition XML. This section lists the User(s) who are permitted access to the UXP Object and the assigned parameters for access. When attributes are defined in the Users section, they apply only the specific User.

Each User (human, machine, or process) is represented and uniquely identified by their User credential set. A User's credential set is referred to as a User Definition prior to it being constructed or imported into the ID Definition XML. A User Definition can be defined simultaneously as the XML is being populated or generated separately using an API process.

An individual User section is organized into the following blocks:

- **Public information** – This section isn't specifically titled using this phrase, but the section is the beginning of each User block with the first attribute being the User name.
- **Private** – This section shows these attributes in their entirety if the User is the Identity owner or someone who has control over the credentials in the User Definition. However, if an Identity is being created on behalf of another User, the User's private attributes will be encrypted within the XML. All private attributes are cloaked and hidden once the ID Definition XML is published. Examples are provided Appendix A.
    - **Rules** – These Rule blocks are defined by and known only to this User. They are access-specific for that User only.
    - **Challenge Pairs** – These are the Prompt/Response sets utilized for authentication. They are private to each User.
- **Rules** – These are User-Level Rule blocks that can be defined by the Identity owner. Once the ID Definition is published, these are cloaked.

3.3.3.3.1 Public Information

The public information attributes are a collection of descriptive details associated to traditional information. Along with this information, there are specific *UXP Identity Privileges* defining the permitted usage of the Identity once the ID Definition XML is published to a UXP Identity. These Privileges along with the public information attributes are described in Table 18.

Figure 10. User Public Attributes in the ID Definition XML

```
<Users>
```

```
<User name="" type="Personal">
  <Enabled type="bool"></Enabled>
  <Email type="string"></Email>
  <Expiration type="date"></Expiration>
  <FormalName type="string"></FormalName>
        <Privileges type="string"></Privileges>
```

Table 18. User Public Attributes in the ID Definition XML

Public Attribute	Datatype	Description
User name	Name	This name identifies this User when the ID Definition XML is published. It isn't necessarily the proper name of the User. The User name issued is discretionary to the User. **Required:** If this attribute is left empty, UXP Technology will generate an error message about this specific attribute in the ID Definition XML. Publication is prevented until this attribute is populated.
Enabled	Boolean	This enables to the User to authenticate into a UXP Object. **Default**: empty or false
Email	String	This is a valid email address associated directly to the User. **Default**: empty
Expiration	Date	Expiration is the date and time when the User is no longer valid and will not be able to authenticate into a UXP Object. Year-Month-DayThour:minute:seconds **Example**: 2121-02-15T18:30:00 The *hour* in the time is measured 0-24.

Public Attribute	Datatype	Description
		If no date and time populates this attribute OR a zero value is defined when the ID Definition XML is published, a default date and time is assigned to this User. **Default**: 100 years from the date of publication **Required*** ***Note**: To prevent getting around this date using time manipulation methods, an additional *Untrusted Time Restriction* attribute can be defined. Section 3.3.4.2.11
FormalName	String	This name is associated with the User. It may be the same as the defined **User name**, but it doesn't need to match if choosing to populate this attribute. **Default:** empty
Privileges	String	These are specific permitted actions regarding UXP Object activity to the individual User once authenticated into the Object. Each User can be assigned different Privileges. **Minimum Privilege Required:** Read The Privileges and their respective actions are listed below: • **Owner** – This is grants all Privileges shown below to the User. • **Read** – This permits the User to read all UXP Object content. • **Write** – This permits the User to write and update UXP Object content. • **Delete** – This permits the User to delete UXP Object content. • **Sign** – This is currently unsupported functionality. • **Read Events** – This permits the logged User to read the embedded UXP Object Event Logs within the

Public Attribute	Datatype	Description
		UXP Object (if the Event Logs are stored within the Object). • **Read Signature** – This is currently unsupported functionality. • **SQL** – This enables this User to utilize UXP SQL within a UXP Object. See UXP Services Guide.

3.3.3.3.2 Private

The private attributes associated with a User have two types of attribute viewing based on the developer's access to the User Definition credentials.

This section shows these attributes in their entirety if the User is the Identity owner or someone who has control over the credentials in the User Definition. However, if an Identity is being created on behalf of another User, the User's private attributes will be encrypted within the XML. All private attributes are cloaked and hidden in the UXP Identity once the ID Definition XML is published. An example is provided Appendix A.

Figure 11. User Private Attributes in the ID Definition XML

```
<Private>
    <Workflow type="bool"></Workflow>
    <Masking type="string"></Masking>
    <!---->
    <HomeConfiguration>
    <Rules>
      <Rule name="UserAdvanced">
        <MaximumTime type="int"></MaximumTime>
        <MaximumTotalTime type="int"></MaximumTotalTime>
        <MinimumTime type="int"></MinimumTime>
        <MinimumTotalTime type="int"></MinimumTotalTime>
      </Rule>
      <!---->
      <Rule name="UserBasic">
        <IgnoreCase type="bool"></IgnoreCase>
```

```
      <IgnoreChars type="string"></IgnoreChars>
      <MinimumPrompts type="int"></MinimumPrompts>
    </Rule>
    <!---->
    <Rule name="UserRecovery">
      <MaximumFailures type="int"></MaximumFailures>
      <MinimumCorrect type="int"></MinimumCorrect>
    </Rule>
  </Rules>
  <!---->
  <Challenges>
    <Challenge name="">
      <Enabled type="bool"></Enabled>
      <Hashed type="bool"></Hashed>
      <Prompt type="string"></Prompt>
      <Required type="bool"></Required>
      <Response type="string"></Response>
      <Softkb type="bool"></Softkb>
    </Challenge>
    <!---->
  </Challenges>
</Private>
```

3.3.3.3.2.1 User Rules

This block consists of advanced attributes specifically applied to a human User who has in-depth understanding of the authentication process. The purpose of these attributes is to make the authentication process for the User more restrictive. The idea behind having a more restrictive authentication process is to prevent an unauthorized person or process from attempting to guess the Responses to the presented Prompts.

The User, in most cases, defines these attributes during the User Definition creation process.

The private User Rules are known only to that User. If the User Definition is imported into the ID Definition XML, these attributes are encrypted. If the developer has access these attributes, then the attributes can be edited as needed.

A machine or process User, in most cases, **NEVER** uses these attributes. The **ONLY** exception is the Workflow attribute.

There are two rule attributes that list individually, *Workflow* and *Masking*. Additionally there is a block titled *HomeConfiguration*.

Figure 12. Private User Attributes: Workflow and Masking

```
<Private>
    <Workflow type="bool"></Workflow>
    <Masking type="string"></Masking>
```

Table 19. Private User Rule Attributes in the ID Definition XML

Private User Attribute	Datatype	Description
Workflow	Boolean	This attribute is for an automated machine workflow. This eliminates human User interaction when a UXP Object is authenticating. **Default**: empty or false
Masking	String	Data masking provides a method for having dynamic Responses during User authentication. The Prompt in each Challenge Pair is presented as expected, but the Response now has an added value that is required in order for the Response to be correct. These added values are time-related, such as *current day* or *current year.* An example is provided below. Masking code values are provided in Table 20. Masking values are defined as a list separated by commas. **Important Note:** Masking and the specific added value are known only to the individual User. The added value to the Response can be placed **before** or **after** the Response. When Masking is enabled, **ALL** Challenge Pairs are included. **Default**: empty or zero, no mask applied.

Example: Masking attribute defining a dynamic Response. The correct Response now has an added value requiring the current year after the Response.

```
<Masking type="string">0,6</Masking>
```

Initial Challenge Pair:

Prompt: trial **Response:** test1

Dynamic Response with the added Mask value:

Response: test12021

Table 20. Masking Value Codes

Masking Value	Code	Code Snippet
`#define MaskUserData`	0	`/*!< Insert user data */` This represents the Response in the Challenge Pair.
`#define MaskAmPm`	1	`/*!< Insert Am or PM */`
`#define MaskHour12`	2	`/*!< Insert current hour */`
`#define MaskHour24`	3	`/*!< Insert current hour */`
`#define MaskDay`	4	`/*!< Insert current day of month */`
`#define MaskMonth`	5	`/*!< Insert current month number */`
`#define MaskYear`	6	`/*!< Insert current year */`
`#define MaskMaxDay`	7	`/*!< Insert number of days in current month */`
`#define MaskLastMonth`	8	`/*!< Insert last month number */`

Masking Value	Code	Code Snippet
#define MaskLastYear	9	/*!< Insert last year */
#define MaskNextMonth	10	/*!< Insert next month number */
#define MaskNextYear	11	/*!< Insert next year */
#define MaskToday	12	/*!< Insert current day of the month */
#define MaskTomorrow	13	/*!< Insert tomorrow day of month */
#define MaskYesterday	14	/*!< Insert yesterday day of month */

Home Configuration: This informational block represents the hardware, location, and network attributes where the User Definition was generated. The attributes are identically structured as other Configurations within the ID Definition XML.

This specific block plays NO ROLE in User validation during authentication and can be removed from the ID Definition XML if desired.

3.3.3.3.2.1.1 User Advanced

The User Advanced attributes are actions associated to the individual User's Responses at authentication. The general focus is establishing a time window in seconds to provide correct Responses to the Prompts presented during authentication.

If these Rule attributes are violated, then the UXP Object denies access without indicating any reason.

These attributes are generally applicable to human User authentication only.

> **Note:** These attributes can be defined individually or as sets. Examples are provided after Table 20.

Figure 13. User Advanced Attributes in the ID Definition XML

```
<Rule name="UserAdvanced">
    <MaximumTime type="int"></MaximumTime>
    <MaximumTotalTime type="int"></MaximumTotalTime>
```

```
    <MinimumTime type="int"></MinimumTime>
    <MinimumTotalTime type="int"></MinimumTotalTime>
</Rule>
```

Table 21. User Advanced Attributes in the ID Definition XML

User Advanced Attribute	Datatype	Description
MaximumTime	Number	This is the maximum time in seconds to **complete** typing each Response before clicking OK to move onto the next presented Prompt. **Default**: 0, indicates no limit
MaximumTotalTime	Number	This is the maximum time in seconds to provide correct Responses and complete authentication into a UXP Object. **Default**: 0, indicates no limit
MinimumTime	Number	This is the minimum number of seconds that is required to pass **before** each Response can begin being typed in. **Default**: 0, indicates no limit
MinimumTotalTime	Number	This is minimum total of seconds that are required to pass before completing authentication with correct Responses. **Default**: 0, indicates no limit

Example 1: MinimumTime = 3 seconds, MaximumTime = 15 seconds. For each Prompt presented, the User must allow 3 seconds to pass ***before*** typing the Response AND ***finish*** the typing of the correct Response and click OK before 15 seconds elapses.

Example 2: MinimumTotalTime = 10 seconds, MaximumTotalTime = 30 seconds. For all Prompts presented, the User must correctly type all Responses ***before*** 30 seconds elapses, BUT the User must NOT finish correctly typing all Responses ***until*** 10 seconds has passed.

3.3.3.3.2.1.2 User Basic

The User Basic attributes focus specifically on the actions of the Challenge Pairs for the individual User during an authentication attempt.

These attributes are generally applicable to human User authentication only.

Figure 14. User Basic Attributes in the ID Definition XML

```
<Rule name="UserBasic">
    <IgnoreCase type="bool"></IgnoreCase>
    <IgnoreChars type="string"></IgnoreChars>
    <MinimumPrompts type="int"></MinimumPrompts>
</Rule>
```

Table 22. User Basic Attributes in the ID Definition XML

User Basic Attribute	Datatype	Description
IgnoreCase	Boolean	The typed Response values, if correct, will match the known Response in the UXP Identity protecting the Object regardless of letter case. **Default**: empty or false
IgnoreChars	String	This specifies any characters that can be ignored in the known Response in the UXP Identity protecting the Object if the User fails to type them in their Response. The UXP Object will consider the Response correct without the characters. **Default**: empty
MinimumPrompts	Number	This designates the minimum number of Challenge Pairs *required for this User* at every authentication attempt into a UXP Object. **Note:** In the Restrictions Rule block, the EveryAuthenticationPrompts attribute is the same parameter and applies to all Users. The parameter with the more restrictive value will be honored regardless of where the parameter is defined. **Default**: 1

3.3.3.3.2.1.3 User Recovery

The User Recovery attributes allow for failed Responses to be bypassed. This is the only mechanism for permitting error-tolerance for human User authentication.

Both attributes must be defined to bypass the failed Response typed by this User in a single authentication session.

These attributes are applicable to human User authentication only.

Figure 15. User Recovery Attributes in the ID Definition XML

```
<Rule name="UserRecovery">
    <MaximumFailures type="int"></MaximumFailures>
    <MinimumCorrect type="int"></MinimumCorrect>
</Rule>
```

Table 23. User Recovery Attributes in the ID Definition XML

User Recovery Attribute	Datatype	Description
MaximumFailures	Number	This number represents how many incorrect Responses are tolerated during a single authentication session. **Default**: empty or zero, indicates all Responses must be answered correctly.
MinimumCorrect	Number	This number represents how many correct Responses are required in a single authentication session. This is only applicable if **MaximumFailures** is greater than zero. **Default**: empty or zero

3.3.3.3.2.2 Challenge Pairs

In the ID Definition XML, the Challenges block houses the Challenge Pairs for the individual User. The Challenge Pairs are the *Prompt/Response* sets. Within the Challenges block, each Prompt/Response set is represented in its own block.

These Prompt/Response sets are a primary contributor to establishing trust for access to a UXP Object. During authentication, the KCL Code uses the Prompt/Response set along with other attributes to validate User access. This validation process applies to all User types, human, machine, or process.

Prompts and Responses are a 1:1 relationship. Each Prompt has a single corresponding Response; this 1:1 relationship is a Challenge Pair.

Challenge Pairs are private and unique to a single User.

The minimum and default number of required Challenge Pairs for User Definition creation is 1. This minimum number can be updated through the API in the system preference **minChallenges.**

Challenge Pairs Role

The KCL Code uses a proprietary algorithm during authentication that performs two significant processes. One process randomizes the Challenge Pair presentment. The other process evaluates and determines the trust level for that User attempting access.

Human User Challenge Pairs

Challenge Pairs in a human User Definition are created manually by the individual User. When constructing the Pairs for human User, UXP Technology promotes using a cognitive approach for the creation process of the Pairs. This cognitive approach focuses on that User's "life experiences".

"Life experiences" are unique as opposed to the conventional challenge-question for a pre-defined, fixed question list. The answers required for this fixed list are discoverable, public details that can be socially reversed-engineered.

"Life experiences" originate from the events only that person had intimate knowledge, connection, and reaction to. To create a Prompt/Response set, a specific "life experience" Prompt is chosen that triggers an immediate memory-trigger Response. These "experience" Prompts leading to memory-triggers are simple and straightforward with little detail.

A memory-trigger Response to an "experience" Prompt share these characteristics:

- Instantaneous (*the same thought occurs every time*)
- Consistent and unambiguous (*the same word or phrase occurs every time*)
- Single word or short phrase

Sertainty recommends avoiding the following Response types:

- Odd spelling, unless the spelling is intentional and consistent
- Pop culture references (*these fluctuate often*)
- Current "favorite" (*e.g. movie, book, food…these may change over time*)

- Long phrases (*these increase the chance of misspelling or forgotten words*)

Examples of Human Prompt/Response Sets

Prompt: Cricket match in Mumbai with Janvi

Response: chai

Prompt: The Jones road-trip to Piccadilly Circus

Response: fries

Machine or Process User Challenge Pairs

For a machine or process, Prompts and Responses are auto-generated by UXP Technology when the User Definition is being created. Each Prompt and its corresponding Response are generated using a random set of 30+ alpha-numeric characters. The Prompt/Response sets are never exposed from the initial generation process all the way through to UXP Identity construction.

Example of Machine or Process Prompt/Response Set

Prompt: <&H%H@PJT_++Y&DS2J&>QP7B08&$}W!G$@)3C

Response: =(U3RL{Z24&LKH?@D[)=$CJRN97%HS#}\Z)M?/R

The Challenge Pairs can securely be embedded in an application utilizing Sertainty Secure Strings.

Sertainty Secure Strings protect the source data on-disk and in-memory preventing pattern matching by binary data scanners.

Figure 16. Challenge Pair Attributes in the ID Definition XML

```
<Challenge name="">
    <Enabled type="bool"></Enabled>
    <Hashed type="bool"></Hashed>
    <Prompt type="string"></Prompt>
    <Required type="bool"></Required>
    <Response type="string"></Response>
    <Softkb type="bool"></Softkb>
</Challenge>
```

Table 24. Challenge Attributes in the ID Definition XML

Challenge Attribute	Datatype	Description
Enabled	Boolean	This activates the Challenge Pair making it available for presentment during authentication into the UXP Object. **Default**: empty or false
Hashed	Boolean	This is a UXP system optimization attribute that is managed by the system.
Prompt	String	This is the presented attribute to the User during authentication. The User must respond with its unique corresponding Response. For a human User, the Prompt itself is discretionary to the User. For a machine or process, the Prompt is auto-generated. **Required**
Required	Boolean	When true, this Challenge Pair **MUST** be presented during authentication. Otherwise, this Pair may or may not be presented during authentication. **Default**: empty or false
Response	String	This is the corresponding attribute for the Prompt in this block. When the Prompt is presented, this is the required Response. For a human User, the Response itself is discretionary to the User. For a machine or process, the Response is auto-generated. **Required**
Softkb	Boolean	This attribute is primarily for human Users who would be authenticating on a device that requires a digital keyboard. **Default**: empty or false

3.3.3.3.3 User-Level Rules

The User-Level Rule blocks are defined for each User in the ID Definition XML by the Identity owner/creator.

The User-Level blocks are the following:

- User Configurations
- User Approvals
- User Schedules

The attributes in these blocks are identical to those of the same title in the ID-Level Rule blocks. As mentioned above, if the same attribute is defined both ID and User-Levels, the more restrictive value is honored.

3.3.3.3.3.1.1 User Configurations

The User Configuration block lists the attributes identically as the attributes shown in the Configurations block at the ID-Level. The three types of information (hardware, location, and network) create the unique *fingerprint* to specify exactly where this User can access a UXP Object.

The necessary User Configuration attributes are created separately using the UXP Configuration function in the respective APIs. This function is an automated process that collects *all attributes* for hardware, location, and network. These attributes are presented in a separate XML document that structurally matches the structure of the ID Definition XML. From this XML, the desired attributes can be included in the User Configurations Rule block with the Identity Definition XML.

A Machine or Process User will have a User Configuration defined to validate its unique fingerprint as well as to indicate where the UXP Object can be accessed.

Post User Configuration Setup Requirements: Once a User Configuration is set up, a Configuration Restriction in the Restrictions Rule block **MUST** be enabled in order for the User Configuration to be fully active. The Configuration Restriction is the resulting UXP Object action if the User Configuration is violated. Without an enabled Configuration Restriction, the Configuration will be ignored.

One or more Configurations can be defined at the global ID and/or User-Levels. (See Appendix A – section 4.2 for an example.)

Figure 17. User Configurations Attributes in the ID Definition XML

```
<Rule name="UserConfigurations">
    <Configurations>
      <Configuration>
        <Id type="int"></Id>
        <Name type="string"></Name>
```

```
<Enabled type="bool"></Enabled>
<!---->
<Device>
  <Id type="int">></Id>
  <Name type="string"></Name>
  <Architecture type="string"></Architecture>
  <CpuModel type="string"></CpuModel>
  <CpuSN type="string"></CpuSN>
  <CpuVendor type="string"></CpuVendor>
  <DeviceType type="string"></DeviceType>
  <MachineModel type="string">></MachineModel>
  <MachineName type="string">></MachineName>
  <MachineSN type="string">></MachineSN>
  <MachineUUID type="string">></MachineUUID>
  <MachineVendor type="string">></MachineVendor>
  <OsFileId type="string">></OsFileId>
  <OsMachine type="string">></OsMachine>
  <OsName type="string">></OsName>
  <OsType type="string">></OsType>
  <OsUserName type="string">></OsUserName>
  <OsVersion type="string">></OsVersion>
  <Ram type="string">></Ram>
  <TimeZone type="string">></TimeZone>
  <TotalMemory type="string">></TotalMemory>
  <Vendor type="string">></Vendor>
</Device>
<!---->
<Location>
  <Id type="int">></Id>
  <Name type="string">></Name>
  <Address type="string">></Address>
  <City type="string">></City>
```

```
          <Country type="string"></Country>
          <InvalidLatitude type="string"></InvalidLatitude>
          <InvalidLongitude type="string"></InvalidLongitude>
          <InvalidRange type="string"></InvalidRange>
          <Latitude type="string"></Latitude>
          <Longitude type="string"></Longitude>
          <Range type="string"></Range>
          <State type="string"></State>
          <Timestamp type="string"></Timestamp>
          <Zipcode type="string"></Zipcode>
        </Location>
        <!---->
        <Network>
          <Id type="int"></Id>
          <Name type="string"></Name>
          <InvalidIp type="string"></InvalidIp>
          <IpAddress type="string"></IpAddress>
        </Network>
      </Configuration>
    </Configurations>
</Rule>
```

An example of a populated Configuration Rule block is located in the Configurations section 3.3.3.2.3.

3.3.3.3.3.1.2 User Approvals

The Users Approvals Rule block is directly associated to human authentication using an external multi-factor authentication (MFA) client. UXP Technology has selected DUO as its current external MFA client. DUO is coded into UXP Technology. This web-based application requires an account with a user to be set up by the customer.

Once the account is set up, specific DUO account details are utilized in configuring a User Approval in this block.

DUO offers a free version along with price-friendly upgraded version. To set up a DUO account, go to https://duo.com/

Figure 18. User Approvals Attributes in the ID Definition XML

```
<Rule name="UserApprovals">
    <ExternalLength type="int"></ExternalLength>
    <Approval name="">
      <Enabled type="bool"></Enabled>
      <Address type="string"></Address>
      <Description type="string"></Description>
      <Prompt type="string"></Prompt>
      <Type type="string">MFA</Type>
      <Response type="string"></Response>
    </Approval>
</Rule>
```

Table 25. User Approvals Attributes in ID Definition XML

User Approval Attribute	Datatype	Description
ExternalLength	Number	This attribute is required for legacy UXP Technology versions 3.4 or lower and is unrelated to the current User Approvals process using DUO. This specifies the number of randomly-generated characters for the User Approval code. This code would be utilized for an email User Approvals process.* ***Note:** In the event that a UXP Object is being authenticated on a legacy version of UXP Technology prior to DUO integration, the User Approval process reverts to sending a User Approval code to a specified email address. This email address is required in the **Address** attribute in this block. **Default:** 6, if User Approval Rule block is enabled
Approval Name	String	This is a unique identifying title or name for the Approval. This attribute doesn't affect the User Approval function using DUO in UXP Technology.

User Approval Attribute	Datatype	Description
		If a name is not defined, then the UXP System defaults to the information in Prompt attribute in this block. **Default:** empty
Enabled	Boolean	This enables the MFA User Approval process. **Default:** empty or false
Address	String	This is an email address. If the UXP Object is authenticating on a legacy version of UXP Technology (3.4 or lower) prior to DUO integration, the Object will send the User Approval code to this email address as an alternative to using DUO.* ***Note:** The **ExternalLength** attribute in this block must contain a number for the Address attribute to be used as an alternative. **Default:** empty
Description	String	This is the content included with the DUO Approval message.* ***Note:** It is recommended to use very specific descriptive information for easy identification of the requestee of the User Approval. **Default:** empty
Prompt	String	This is the specific Prompt connected to this User Approval and is included with the DUO Approval request.* The Prompt is **required** for using DUO for UXP Object authentication. ***Note:** It is recommended to make the Prompt very specific for easy identification of the requestee of the User Approval. **Default:** empty
Type	String	This defines the method of the User Approval configuration and the delivery mechanism. **Required**

User Approval Attribute	Datatype	Description
		Type: MFA
Response	String	The specific DUO User information is used in this string attribute. Response is a **required** attribute. The DUO account components used in the Response attribute are the following: • **Username** – This is set up in the DUO account. • **Integration key** – This is auto-generated by DUO for the user account. • **Secret key** – This is auto-generated by DUO for the user account. • **API hostname** – This is the URL that tells the UXP System how to communicate with DUO. • **Timeout** – This is a value in *seconds* indicating how long the UXP System will wait for DUO to respond to the User Approval request sent to DUO by the UXP Object. If the time passes before DUO responds, the UXP Object denies access without indicating a reason. **Default:** 30 seconds These components are placed in a specific order in the Response attribute and are shown below. **Response String:** DUO:Username:IntegrationKey:SecretKey:APIhostname:Timeout See Appendix A – section 4.3 for an example.

3.3.3.3.3.1.3 User Schedule

User Schedule attributes define a day of the week and/or specific time-window when access is permitted to a UXP Object. When a User Schedule is set up, the time-window and/or day is the ONLY time that a UXP Object can be accessed.

For a time-window User Schedule, *a Start and End attribute must be defined*. If either a Start or End attribute is defined without an opposing attribute defined to create a time-window, UXP Technology recognizes the missing attribute. The Technology responds by populating the missing attribute with the *current date and/or time.**

> ***Note:** This scenario may cause a date/time mis-match. The mis-match results in an invalid ID Definition XML, and publication will be prevented.

Start /End Attributes: All attributes require population in both the Start and End category. If only one attribute is populated, then UXP Technology will automatically fill in the empty attributes with the current date/time information. This may cause a date/time mis-match as noted above and create problems with publications.

Post User Schedule Setup Requirements: Once a User Schedule is set up, a Schedule Restriction in the Restrictions Rule block **MUST** be enabled in order for the Schedule to be fully active. The Schedule Restriction is the resulting UXP Object action if the User Schedule is violated. Without an enabled Schedule Restriction, the Schedule will be ignored.

A Schedule can be defined at the global ID and/or User-Levels.

Figure 19. User Schedule Attributes in the ID Definition XML

```
<Rule name="UserSchedule">
    <Enabled type="bool"></Enabled>
    <DaySunday type="bool"></DaySunday>
    <DayMonday type="bool"></DayMonday>
    <DayTuesday type="bool"></DayTuesday>
    <DayWednesday type="bool"></DayWednesday>
    <DayThursday type="bool"></DayThursday>
    <DayFriday type="bool"></DayFriday>
    <DaySaturday type="bool"></DaySaturday>
    <StartDay type="int"></StartDay>
    <StartHour type="int"></StartHour>
    <StartMinute type="int"></StartMinute>
    <StartMonth type="int"></StartMonth>
    <StartYear type="int"></StartYear>
    <EndDay type="int"></EndDay>
    <EndHour type="int"></EndHour>
    <EndMinute type="int"></EndMinute>
```

```
    <EndMonth type="int"></EndMonth>
    <EndYear type="int"></EndYear>
</Rule>
```

Table 26. User Schedule Attributes in ID Definition XML

User Schedule Attribute	Datatype	Description
Enabled	Boolean	This is enables the defined User Schedule. **Default:** empty
DaySunday	Boolean	**True:** UXP Object access on Sunday is permitted.
DayMonday	Boolean	**True:** UXP Object access on Monday is permitted.
DayTuesday	Boolean	**True:** UXP Object access on Tuesday is permitted.
DayWednesday	Boolean	**True:** UXP Object access on Wednesday is permitted.
DayThursday	Boolean	**True:** UXP Object access on Thursday is permitted.
DayFriday	Boolean	**True:** UXP Object access on Friday is permitted.
DaySaturday	Boolean	**True:** UXP Object access on Saturday is permitted.
StartDay	Number	This specifies the day of the month on which **UXP Object** access starts. **Default:** -1 indicates any day
StartHour	Number	This specifies the hour of the day on which **UXP Object** access starts. **Default:** -1 indicates any hour

User Schedule Attribute	Datatype	Description
StartMinute	Number	This specifies the minute of the hour on which **UXP Object** access starts. **Default:** -1 indicates any minute
StartMonth	Number	This specifies the month of the year on which **UXP Object** access starts. **Default:** -1 indicates any month
StartYear	Number	This specifies the year on which **UXP Object** access starts. **Default:** -1 indicates any year
EndDay	Number	This specifies the day of the month on which **UXP Object** access ends. **Default:** -1 indicates any day
EndHour	Number	This specifies the hour of the day on which **UXP Object** access ends. **Default:** -1 indicates any hour
EndMinute	Number	This specifies the minute of the hour on which **UXP Object** access ends. **Default:** -1 indicates any minute
EndMonth	Number	This specifies the month of the year on which **UXP Object** access ends. **Default:** -1 indicates any month
EndYear	Number	This specifies the year on which **UXP Object** access ends.

User Schedule Attribute	Datatype	Description
		Default: -1 indicates any year

4 Appendix A – XML Examples

4.1 ID Definition XML Template

Shown below is the ID Definition XML Template containing the *all available attributes*. As stated in the sections above, not all attributes need to be included to publish to a UXP Identity file. If minimum publishing requirements aren't met, then the UXP Technology system will throw an error indicating which attribute needs to be defined.

Example: ID Definition XML Template

```
<?xml version="1.0"?>
<!---->
<!-- ID Definition: Name-of-xml -->
<!---->
<!-- Date: 2021-03-11T16:16:39 -->
<!---->
<ID name="Name-of-xml">
  <Description type="string"></Description>
  <Expiration type="date"></Expiration>
  <PersonalName1 type="string"></PersonalName1>
  <PersonalName2 type="string"></PersonalName2>
  <PersonalName3 type="string"></PersonalName3>
  <Address1 type="string"></Address1>
  <Address2 type="string"></Address2>
  <City type="string"></City>
  <State type="string"></State>
  <Zipcode type="string"></Zipcode>
  <Country type="string"></Country>
  <Privileges type="string"></Privileges>
  <!---->
  <Rules>
    <Rule name="Access">
      <AdvancedDataLogging type="bool"></AdvancedDataLogging>
      <Compliance type="int"></Compliance>
      <MaximumAccesses type="int"></MaximumAccesses>
      <MaximumCycleFailures type="int"></MaximumCycleFailures>
      <MaximumIdleTime type="int"></MaximumIdleTime>
      <MaximumTotalFailures type="int"></MaximumTotalFailures>
      <UseLocalTime type="bool"></UseLocalTime>
      <Workflow type="bool"></Workflow>
    </Rule>
    <!---->
    <Rule name="Restrictions">
      <ConfigurationApproval type="bool"></ConfigurationApproval>
      <ConfigurationDeny type="bool"></ConfigurationDeny>
      <ConfigurationDestroy type="bool"></ConfigurationDestroy>
      <ConfigurationPrompts type="int"></ConfigurationPrompts>
      <EveryAuthenticationApproval type="bool"></EveryAuthenticationApproval>
      <EveryAuthenticationPrompts type="int"></EveryAuthenticationPrompts>
      <HardwareApproval type="bool"></HardwareApproval>
      <HardwareDeny type="bool"></HardwareDeny>
      <HardwareDestroy type="bool"></HardwareDestroy>
      <HardwarePrompts type="int"></HardwarePrompts>
      <LocationApproval type="bool"></LocationApproval>
      <LocationDeny type="bool"></LocationDeny>
```

```
    <LocationDestroy type="bool"></LocationDestroy>
    <LocationPrompts type="int"></LocationPrompts>
    <MovementApproval type="bool"></MovementApproval>
    <MovementDeny type="bool"></MovementDeny>
    <MovementDestroy type="bool"></MovementDestroy>
    <MovementPrompts type="int"></MovementPrompts>
    <NetworkApproval type="bool"></NetworkApproval>
    <NetworkDeny type="bool"></NetworkDeny>
    <NetworkDestroy type="bool"></NetworkDestroy>
    <NetworkPrompts type="int"></NetworkPrompts>
    <Preset type="string"></Preset>
    <ScheduleApproval type="bool"></ScheduleApproval>
    <ScheduleDeny type="bool"></ScheduleDeny>
    <ScheduleDestroy type="bool"></ScheduleDestroy>
    <SchedulePrompts type="int"></SchedulePrompts>
    <UntrustedSystemApproval type="bool"></UntrustedSystemApproval>
    <UntrustedSystemDeny type="bool"></UntrustedSystemDeny>
    <UntrustedSystemDestroy type="bool"></UntrustedSystemDestroy>
    <UntrustedSystemPrompts type="int"></UntrustedSystemPrompts>
    <UntrustedTimeApproval type="bool"></UntrustedTimeApproval>
    <UntrustedTimeDeny type="bool"></UntrustedTimeDeny>
    <UntrustedTimeDestroy type="bool"></UntrustedTimeDestroy>
    <UntrustedTimePrompts type="int"></UntrustedTimePrompts>
  </Rule>
  <!---->
  <Rule name="Configurations">
    <Configurations>
      <Configuration>
        <Id type="int"></Id>
        <Name type="string"></Name>
        <Enabled type="bool"></Enabled>
        <!---->
        <Device>
          <Id type="int"></Id>
          <Name type="string"></Name>
          <Architecture type="string"></Architecture>
          <CpuModel type="string"></CpuModel>
          <CpuSN type="string"></CpuSN>
          <CpuVendor type="string"></CpuVendor>
          <DeviceType type="string"></DeviceType>
          <MachineModel type="string"></MachineModel>
          <MachineName type="string"></MachineName>
          <MachineSN type="string"></MachineSN>
          <MachineUUID type="string"></MachineUUID>
          <MachineVendor type="string"></MachineVendor>
          <OsFileId type="string"></OsFileId>
          <OsMachine type="string"></OsMachine>
          <OsName type="string"></OsName>
          <OsType type="string"></OsType>
          <OsUserName type="string"></OsUserName>
          <OsVersion type="string"></OsVersion>
          <Ram type="string"></Ram>
          <TimeZone type="string"></TimeZone>
          <TotalMemory type="string"></TotalMemory>
          <Vendor type="string"></Vendor>
        </Device>
        <!---->
        <Location>
          <Id type="int"></Id>
          <Name type="string"></Name>
          <Address type="string"></Address>
          <City type="string"></City>
          <Country type="string"></Country>
          <InvalidLatitude type="string"></InvalidLatitude>
          <InvalidLongitude type="string"></InvalidLongitude>
          <InvalidRange type="string"></InvalidRange>
          <Latitude type="string"></Latitude>
          <Longitude type="string"></Longitude>
          <Range type="string"></Range>
          <State type="string"></State>
          <Timestamp type="string"></Timestamp>
          <Zipcode type="string"></Zipcode>
        </Location>
        <!---->
        <Network>
          <Id type="int"></Id>
          <Name type="string"></Name>
          <InvalidIp type="string"></InvalidIp>
```

```
            <IpAddress type="string"></IpAddress>
          </Network>
        </Configuration>
      </Configurations>
    </Rule>
    <!---->
    <Rule name="Alerts">
      <EmailAddress type="string"></EmailAddress>
      <IncludeDevice type="bool"></IncludeDevice>
      <IncludeLicense type="bool"></IncludeLicense>
      <IncludeLocation type="bool"></IncludeLocation>
      <SMSAddress type="string"></SMSAddress>
      <UseEmail type="bool"></UseEmail>
      <UseSMS type="bool"></UseSMS>
    </Rule>
    <!---->
    <Rule name="Approvals">
      <ExternalLength type="int"></ExternalLength>
      <Approval name="">
        <Enabled type="bool"></Enabled>
        <Address type="string"></Address>
        <Description type="string"></Description>
        <Prompt type="string"></Prompt>
        <Type type="string"></Type>
        <Response type="string"></Response>
      </Approval>
    </Rule>
    <!---->
    <Rule name="Events">
      <EmailAddress type="string"></EmailAddress>
      <ExternalKey type="string"></ExternalKey>
      <FileSpec type="string"></FileSpec>
      <LogAccesses type="bool"></LogAccesses>
      <LogCustom type="bool"></LogCustom>
      <LogFailures type="bool"></LogFailures>
      <LogMessages type="bool"></LogMessages>
      <LogRepeats type="bool"></LogRepeats>
      <RecordEmail type="bool"></RecordEmail>
      <RecordExternal type="bool"></RecordExternal>
      <RecordFile type="bool"></RecordFile>
      <RecordLocal type="bool"></RecordLocal>
      <RecordRemote type="bool"></RecordRemote>
      <RecordSMS type="bool"></RecordSMS>
      <RemoteURL type="string"></RemoteURL>
      <SMSAddress type="string"></SMSAddress>
    </Rule>
    <!---->
    <Rule name="Schedule">
      <Enabled type="bool"></Enabled>
      <DaySunday type="bool"></DaySunday>
      <DayMonday type="bool"></DayMonday>
      <DayTuesday type="bool"></DayTuesday>
      <DayWednesday type="bool"></DayWednesday>
      <DayThursday type="bool"></DayThursday>
      <DayFriday type="bool"></DayFriday>
      <DaySaturday type="bool"></DaySaturday>
      <StartDay type="int"></StartDay>
      <StartHour type="int"></StartHour>
      <StartMinute type="int"></StartMinute>
      <StartMonth type="int"></StartMonth>
      <StartYear type="int"></StartYear>
      <EndDay type="int"></EndDay>
      <EndHour type="int"></EndHour>
      <EndMinute type="int"></EndMinute>
      <EndMonth type="int"></EndMonth>
      <EndYear type="int"></EndYear>
    </Rule>
  </Rules>
  <!---->
  <Users>
    <User name="" type="Personal">
      <Enabled type="bool"></Enabled>
      <Email type="string"></Email>
      <Expiration type="date"></Expiration>
      <FormalName type="string"></FormalName>
      <Privileges type="string"></Privileges>
      <!---->
      <Private>
```

```
    <Workflow type="bool"></Workflow>
    <Masking type="string"></Masking>
    <!---->
    <Rules>
      <Rule name="UserAdvanced">
        <MaximumTime type="int"></MaximumTime>
        <MaximumTotalTime type="int"></MaximumTotalTime>
        <MinimumTime type="int"></MinimumTime>
        <MinimumTotalTime type="int"></MinimumTotalTime>
      </Rule>
      <!---->
      <Rule name="UserBasic">
        <IgnoreCase type="bool"></IgnoreCase>
        <IgnoreChars type="string"></IgnoreChars>
        <MinimumPrompts type="int"></MinimumPrompts>
      </Rule>
      <!---->
      <Rule name="UserRecovery">
        <MaximumFailures type="int"></MaximumFailures>
        <MinimumCorrect type="int"></MinimumCorrect>
      </Rule>
    </Rules>
    <!---->
    <Challenges>
      <Challenge name="">
        <Enabled type="bool"></Enabled>
        <Hashed type="bool"></Hashed>
        <Prompt type="string"></Prompt>
        <Required type="bool"></Required>
        <Response type="string"></Response>
        <Softkb type="bool"></Softkb>
      </Challenge>
      <!---->
    </Challenges>
  </Private>
  <!---->
  <Rules>
    <Rule name="UserConfigurations">
      <Configurations>
        <Configuration>
          <Id type="int"></Id>
          <Name type="string"></Name>
          <Enabled type="bool"></Enabled>
          <!---->
          <Device>
            <Id type="int"></Id>
            <Name type="string"></Name>
            <Architecture type="string"></Architecture>
            <CpuModel type="string"></CpuModel>
            <CpuSN type="string"></CpuSN>
            <CpuVendor type="string"></CpuVendor>
            <DeviceType type="string"></DeviceType>
            <MachineModel type="string"></MachineModel>
            <MachineName type="string"></MachineName>
            <MachineSN type="string"></MachineSN>
            <MachineUUID type="string"></MachineUUID>
            <MachineVendor type="string"></MachineVendor>
            <OsFileId type="string"></OsFileId>
            <OsMachine type="string"></OsMachine>
            <OsName type="string"></OsName>
            <OsType type="string"></OsType>
            <OsUserName type="string"></OsUserName>
            <OsVersion type="string"></OsVersion>
            <Ram type="string"></Ram>
            <TimeZone type="string"></TimeZone>
            <TotalMemory type="string"></TotalMemory>
            <Vendor type="string"></Vendor>
          </Device>
          <!---->
          <Location>
            <Id type="int"></Id>
            <Name type="string"></Name>
            <Address type="string"></Address>
            <City type="string"></City>
            <Country type="string"></Country>
            <InvalidLatitude type="string"></InvalidLatitude>
            <InvalidLongitude type="string"></InvalidLongitude>
            <InvalidRange type="string"></InvalidRange>
```

```
                <Latitude type="string"></Latitude>
                <Longitude type="string"></Longitude>
                <Range type="string"></Range>
                <State type="string"></State>
                <Timestamp type="string"></Timestamp>
                <Zipcode type="string"></Zipcode>
              </Location>
              <!---->
              <Network>
                <Id type="int"></Id>
                <Name type="string"></Name>
                <InvalidIp type="string"></InvalidIp>
                <IpAddress type="string"></IpAddress>
              </Network>
            </Configuration>
          </Configurations>
        </Rule>
        <!---->
        <Rule name="UserApprovals">
          <ExternalLength type="int"></ExternalLength>
          <Approval name="">
            <Enabled type="bool"></Enabled>
            <Address type="string"></Address>
            <Description type="string"></Description>
            <Prompt type="string"></Prompt>
            <Type type="string"></Type>
            <Response type="string"></Response>
          </Approval>
        </Rule>
        <!---->
        <Rule name="UserSchedule">
          <Enabled type="bool"></Enabled>
          <DaySunday type="bool"></DaySunday>
          <DayMonday type="bool"></DayMonday>
          <DayTuesday type="bool"></DayTuesday>
          <DayWednesday type="bool"></DayWednesday>
          <DayThursday type="bool"></DayThursday>
          <DayFriday type="bool"></DayFriday>
          <DaySaturday type="bool"></DaySaturday>
          <StartDay type="int"></StartDay>
          <StartHour type="int"></StartHour>
          <StartMinute type="int"></StartMinute>
          <StartMonth type="int"></StartMonth>
          <StartYear type="int"></StartYear>
          <EndDay type="int"></EndDay>
          <EndHour type="int"></EndHour>
          <EndMinute type="int"></EndMinute>
          <EndMonth type="int"></EndMonth>
          <EndYear type="int"></EndYear>
        </Rule>
      </Rules>
    </User>
  </Users>
</ID>
```


4.2 Multiple Configurations

Below shows the ID-Level Configurations Rule block populated with three Configurations.

The attribute details are collected using an automated UXP Technology function call from the respective API. These attributes are identical for ID and User-Level Configurations Rule blocks.


```
<Configurations>
  <Configuration>
    <Id type="int">2777075048</Id>
    <Name type="string">Chicago-IL-N-172.58.136.31</Name>
    <Enabled type="bool">true</Enabled>
    <!---->
    <Device>
      <Id type="int">1665407208</Id>
      <Name type="string">xxo-Test1-MacBook-Pro-2.local</Name>
      <Architecture type="string">x86_64</Architecture>
```

```
      <CpuModel type="string">Intel(R) Core(TM) i9-9050HK CPU @ 2.90GHz</CpuModel>
      <CpuSN type="string"></CpuSN>
      <CpuVendor type="string">GenuineIntel</CpuVendor>
      <DeviceType type="string">Mobile Device</DeviceType>
      <MachineModel type="string">MacBookPro15,1</MachineModel>
      <MachineName type="string">Test1-MacBook-Pro-2.local</MachineName>
      <MachineSN type="string">C02XT023JGH7</MachineSN>
      <MachineUUID type="string">589E4C46-9682-5759-BBCA-47A6561C3CA7</MachineUUID>
      <MachineVendor type="string">Apple</MachineVendor>
      <OsFileId type="string">32cf5e458630d</OsFileId>
      <OsMachine type="string">x86_64</OsMachine>
      <OsName type="string">MacOSX</OsName>
      <OsType type="string">Mac OS X</OsType>
      <OsUserName type="string">msw</OsUserName>
      <OsVersion type="string">10.15.7</OsVersion>
      <Ram type="string">16384</Ram>
      <TimeZone type="string">-360</TimeZone>
      <TotalMemory type="string">17179869184</TotalMemory>
      <Vendor type="string">Apple</Vendor>
    </Device>
    <!---->
    <Location>
      <Id type="int">414998389</Id>
      <Name type="string">Chicago-IL</Name>
      <Address type="string">5000 S Homan Ave</Address>
      <City type="string">Chicago</City>
      <Country type="string">US</Country>
      <InvalidLatitude type="string">0.000</InvalidLatitude>
      <InvalidLongitude type="string">0.000</InvalidLongitude>
      <InvalidRange type="string">0.000</InvalidRange>
      <Latitude type="string">35.804</Latitude>
      <Longitude type="string">-90.707</Longitude>
      <Range type="string">0.000</Range>
      <State type="string">IL</State>
      <Timestamp type="string">Wed Dec 31 18:00:00 1969</Timestamp>
      <Zipcode type="string">60632</Zipcode>
    </Location>
    <!---->
    <Network>
      <Id type="int">3794685721</Id>
      <Name type="string">N-172.78.136.31</Name>
      <InvalidIp type="string"></InvalidIp>
      <IpAddress type="string">172.78.136.31</IpAddress>
    </Network>
  </Configuration>
  <!---->
  <Configuration>
    <Id type="int">3077663052</Id>
    <Name type="string">ColumbiaTN-xxc-Test2-MBP-2</Name>
    <Enabled type="bool">false</Enabled>
    <!---->
    <Device>
      <Id type="int">1665407208</Id>
      <Name type="string">xxc-Test2-MBP-2</Name>
      <Architecture type="string"></Architecture>
      <CpuModel type="string"></CpuModel>
      <CpuSN type="string"></CpuSN>
      <CpuVendor type="string"></CpuVendor>
      <DeviceType type="string"></DeviceType>
      <MachineModel type="string"></MachineModel>
      <MachineName type="string"></MachineName>
      <MachineSN type="string"></MachineSN>
      <MachineUUID type="string"></MachineUUID>
      <MachineVendor type="string"></MachineVendor>
      <OsFileId type="string"></OsFileId>
      <OsMachine type="string"></OsMachine>
      <OsName type="string"></OsName>
      <OsType type="string"></OsType>
      <OsUserName type="string"></OsUserName>
      <OsVersion type="string"></OsVersion>
      <Ram type="string"></Ram>
      <TimeZone type="string"></TimeZone>
      <TotalMemory type="string"></TotalMemory>
      <Vendor type="string"></Vendor>
    </Device>
    <!---->
    <Location>
      <Id type="int">186256501</Id>
```

```
      <Name type="string">FranklinTN</Name>
      <Address type="string"></Address>
      <City type="string"></City>
      <InvalidLatitude type="string">0.000</InvalidLatitude>
      <InvalidLongitude type="string">0.000</InvalidLongitude>
      <InvalidRange type="string">0.000</InvalidRange>
      <Latitude type="string"></Latitude>
      <Longitude type="string"></Longitude>
      <Range type="string">0.000</Range>
      <ScoreAddress type="string"></ScoreAddress>
      <ScoreCity type="string"></ScoreCity>
      <ScoreCountry type="string"></ScoreCountry>
      <ScoreState type="string"></ScoreState>
      <ScoreZipcode type="string"></ScoreZipcode>
      <State type="string"></State>
      <Timestamp type="string">Wed Dec 31 18:00:00 1969</Timestamp>
      <Zipcode type="string"></Zipcode>
    </Location>
    <!---->
    <Network>
      <Id type="int">0</Id>
      <Name type="string"></Name>
      <InvalidIp type="string"></InvalidIp>
      <IpAddress type="string"></IpAddress>
      <ScoreIP type="string"></ScoreIP>
    </Network>
  </Configuration>
  <!---->
  <Configuration>
    <Id type="int">655740300</Id>
    <Name type="string">Nashville-TN-N-99.106.46.121</Name>
    <Enabled type="bool">false</Enabled>
    <!---->
    <Device>
      <Id type="int">1665407208</Id>
      <Name type="string">xxx-Test-MBP-2.attlocal.net</Name>
      <Architecture type="string">x86_64</Architecture>
      <CpuModel type="string">Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz</CpuModel>
      <CpuSN type="string"></CpuSN>
      <CpuVendor type="string">GenuineIntel</CpuVendor>
      <DeviceType type="string">Mobile Device</DeviceType>
      <MachineModel type="string">MacBookPro15,1</MachineModel>
      <MachineName type="string">Test-MBP-2.attlocal.net</MachineName>
      <MachineSN type="string">C02XT986JGH7</MachineSN>
      <MachineUUID type="string">575E8C46-9682-5759-BBCA-47A6561C3CA7</MachineUUID>
      <MachineVendor type="string">Apple</MachineVendor>
      <OsFileId type="string">32cf6e338630d</OsFileId>
      <OsMachine type="string">x86_64</OsMachine>
      <OsName type="string">MacOSX</OsName>
      <OsType type="string">Mac OS X</OsType>
      <OsUserName type="string">msw</OsUserName>
      <OsVersion type="string">10.15.7</OsVersion>
      <Ram type="string">16384</Ram>
      <TimeZone type="string">-360</TimeZone>
      <TotalMemory type="string">17179869184</TotalMemory>
      <Vendor type="string">Apple</Vendor>
    </Device>
    <!---->
    <Location>
      <Id type="int">1239596164</Id>
      <Name type="string">Nashville-TN</Name>
      <Address type="string">712 Hyper Rd</Address>
      <City type="string">Nashville</City>
      <Country type="string">US</Country>
      <InvalidLatitude type="string">0.000</InvalidLatitude>
      <InvalidLongitude type="string">0.000</InvalidLongitude>
      <InvalidRange type="string">0.000</InvalidRange>
      <Latitude type="string">36.589</Latitude>
      <Longitude type="string">-87.697</Longitude>
      <Range type="string">0.000</Range>
      <ScoreAddress type="string"></ScoreAddress>
      <ScoreCity type="string"></ScoreCity>
      <ScoreCountry type="string"></ScoreCountry>
      <ScoreState type="string"></ScoreState>
      <ScoreZipcode type="string"></ScoreZipcode>
      <State type="string">TN</State>
      <Timestamp type="string">Wed Dec 31 18:00:00 1969</Timestamp>
      <Zipcode type="string">37125</Zipcode>
```

```
          </Location>
          <!---->
          <Network>
            <Id type="int">594800945</Id>
            <Name type="string">N-99.109.46.121</Name>
            <InvalidIp type="string"></InvalidIp>
            <IpAddress type="string">99.106.46.131</IpAddress>
            <ScoreIP type="string"></ScoreIP>
          </Network>
        </Configuration>

      </Configurations>
```

4.3 DUO MFA Approval

Below shows the ID-Level Approvals Rule block populated with DUO MFA components.

The attribute details are collected using an automated UXP Technology function call from the respective API. These attributes are identical for ID and User-Level Approvals Rule blocks.

```
    <Rule name="Approvals">
      <ExternalLength type="int">6</ExternalLength>
      <Approval name="DUO approval required from test1">
        <Enabled type="bool">true</Enabled>
        <Address type="string">test1@sertainty.com</Address>
        <Description type="string">Testing DUO details</Description>
        <Prompt type="string">DUO approval required from test1</Prompt>
        <Type type="string">MFA</Type>
        <Response type="string">DUO:test1-
work:DIQOITXLJOJO65N3KJC8:5YUIbs0fKwnQhz5m0cwp9llVRfFpav150TbU0TAN:api-1e29e25b.duosecurity.com:30</Response>
      </Approval>

    </Rule>
```

4.4 Imported Users with Private Details Encrypted

This is the Users section in the ID Definition XML containing multiple Users (Workgroup). The Workgroup represent both human and machine Users. Three are human (one owner/creator, two imported), and two are machine. One machine is associated to the owner, and the second machine is imported.

```
      <Users>
         <User name="UserTest1" type="Trusted">
           <Enabled type="bool">true</Enabled>
           <Email type="string">UserTest1@sertainty.com</Email>
           <Expiration type="date">2120-02-03T18:00:00</Expiration>
           <FormalName type="string">UserTest1</FormalName>
           <Reality type="string"></Reality>
           <Privileges type="string">Read,Write,ReadSignature</Privileges>
           <!---->
           <Private>...encoded-user-data...</Private>
           <!---->
           <Rules>
             <Rule name="UserConfigurations">
               <Configurations />
             </Rule>
             <!---->
             <Rule name="UserApprovals">
               <ExternalLength type="int">6</ExternalLength>
             </Rule>
             <!---->
             <Rule name="UserSchedule">
               <Enabled type="bool">true</Enabled>
               <DaySunday type="bool">true</DaySunday>
               <DayMonday type="bool">true</DayMonday>
               <DayTuesday type="bool">true</DayTuesday>
```

```
        <DayWednesday type="bool">true</DayWednesday>
        <DayThursday type="bool">true</DayThursday>
        <DayFriday type="bool">true</DayFriday>
        <DaySaturday type="bool">true</DaySaturday>
        <StartDay type="int">-1</StartDay>
        <StartHour type="int">-1</StartHour>
        <StartMinute type="int">-1</StartMinute>
        <StartMonth type="int">-1</StartMonth>
        <StartYear type="int">-1</StartYear>
        <EndDay type="int">-1</EndDay>
        <EndHour type="int">-1</EndHour>
        <EndMinute type="int">-1</EndMinute>
        <EndMonth type="int">-1</EndMonth>
        <EndYear type="int">-1</EndYear>
      </Rule>
    </Rules>
  </User>
  <!---->
  <User name="UserTest2" type="Trusted">
    <Enabled type="bool">true</Enabled>
    <Email type="string">UserTest2@hotmail.com</Email>
    <Expiration type="date">2120-02-03T18:00:00</Expiration>
    <FormalName type="string">UserTest2</FormalName>
    <Reality type="string"></Reality>
    <Privileges type="string">Read,Write,Delete</Privileges>
    <!---->
    <Private>...encoded-user-data...</Private>
    <!---->
    <Rules>
      <Rule name="UserConfigurations">
        <Configurations />
      </Rule>
      <!---->
      <Rule name="UserApprovals">
        <ExternalLength type="int">6</ExternalLength>
      </Rule>
      <!---->
      <Rule name="UserSchedule">
        <Enabled type="bool">false</Enabled>
        <DaySunday type="bool">true</DaySunday>
        <DayMonday type="bool">true</DayMonday>
        <DayTuesday type="bool">true</DayTuesday>
        <DayWednesday type="bool">true</DayWednesday>
        <DayThursday type="bool">true</DayThursday>
        <DayFriday type="bool">true</DayFriday>
        <DaySaturday type="bool">true</DaySaturday>
        <StartDay type="int">-1</StartDay>
        <StartHour type="int">-1</StartHour>
        <StartMinute type="int">-1</StartMinute>
        <StartMonth type="int">-1</StartMonth>
        <StartYear type="int">-1</StartYear>
        <EndDay type="int">-1</EndDay>
        <EndHour type="int">-1</EndHour>
        <EndMinute type="int">-1</EndMinute>
        <EndMonth type="int">-1</EndMonth>
        <EndYear type="int">-1</EndYear>
      </Rule>
    </Rules>
  </User>
  <!---->
  <User name="mich" type="Personal">
    <Enabled type="bool">true</Enabled>
    <Email type="string">mich@sertainty.com</Email>
    <Expiration type="date">2120-02-03T18:00:00</Expiration>
    <FormalName type="string">Mich</FormalName>
    <Reality type="string"></Reality>
    <Privileges type="string">Read,Write,Owner</Privileges>
    <!---->
    <Private>
      <Workflow type="bool">false</Workflow>
      <Masking type="string">0</Masking>
      <!---->
      <Rules>
        <Rule name="UserAdvanced">
          <MaximumTime type="int">60</MaximumTime>
          <MaximumTotalTime type="int">60</MaximumTotalTime>
          <MinimumTime type="int">0</MinimumTime>
          <MinimumTotalTime type="int">0</MinimumTotalTime>
```

```
    </Rule>
    <!---->
    <Rule name="UserBasic">
      <IgnoreCase type="bool">true</IgnoreCase>
      <IgnoreChars type="string"></IgnoreChars>
      <MinimumPrompts type="int">3</MinimumPrompts>
    </Rule>
    <!---->
    <Rule name="UserPanic">
      <Panic type="string"></Panic>
      <PanicEmail type="string"></PanicEmail>
      <PanicSMS type="string"></PanicSMS>
    </Rule>
    <!---->
    <Rule name="UserRecovery">
      <MaximumFailures type="int">0</MaximumFailures>
      <MinimumCorrect type="int">6</MinimumCorrect>
    </Rule>
  </Rules>
  <!---->
  <Challenges>
    <Challenge name="eight">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">eight</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">nine</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="five">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">five</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">six</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="four">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">four</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">five</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="nine">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">nine</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">ten</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="one">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">one</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">two</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="seven7">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
      <Prompt type="string">seven7</Prompt>
      <Required type="bool">false</Required>
      <Response type="string">eight</Response>
      <Softkb type="bool">false</Softkb>
    </Challenge>
    <!---->
    <Challenge name="six">
      <Enabled type="bool">true</Enabled>
      <Hashed type="bool">false</Hashed>
```

```
          <Prompt type="string">six</Prompt>
          <Required type="bool">false</Required>
          <Response type="string">seven</Response>
          <Softkb type="bool">false</Softkb>
        </Challenge>
        <!---->
        <Challenge name="ten">
          <Enabled type="bool">true</Enabled>
          <Hashed type="bool">false</Hashed>
          <Prompt type="string">ten</Prompt>
          <Required type="bool">false</Required>
          <Response type="string">eleven</Response>
          <Softkb type="bool">false</Softkb>
        </Challenge>
        <!---->
        <Challenge name="three">
          <Enabled type="bool">true</Enabled>
          <Hashed type="bool">false</Hashed>
          <Prompt type="string">three</Prompt>
          <Required type="bool">false</Required>
          <Response type="string">four</Response>
          <Softkb type="bool">false</Softkb>
        </Challenge>
        <!---->
        <Challenge name="two">
          <Enabled type="bool">true</Enabled>
          <Hashed type="bool">false</Hashed>
          <Prompt type="string">two</Prompt>
          <Required type="bool">false</Required>
          <Response type="string">three</Response>
          <Softkb type="bool">false</Softkb>
        </Challenge>
      </Challenges>
    </Private>
    <!---->
    <Rules>
      <Rule name="UserConfigurations">
        <Configurations />
      </Rule>
      <!---->
      <Rule name="UserApprovals">
        <ExternalLength type="int">6</ExternalLength>
      </Rule>
      <!---->
      <Rule name="UserSchedule">
        <Enabled type="bool">false</Enabled>
        <DaySunday type="bool">true</DaySunday>
        <DayMonday type="bool">true</DayMonday>
        <DayTuesday type="bool">true</DayTuesday>
        <DayWednesday type="bool">true</DayWednesday>
        <DayThursday type="bool">true</DayThursday>
        <DayFriday type="bool">true</DayFriday>
        <DaySaturday type="bool">true</DaySaturday>
        <StartDay type="int">-1</StartDay>
        <StartHour type="int">-1</StartHour>
        <StartMinute type="int">-1</StartMinute>
        <StartMonth type="int">-1</StartMonth>
        <StartYear type="int">-1</StartYear>
        <EndDay type="int">-1</EndDay>
        <EndHour type="int">-1</EndHour>
        <EndMinute type="int">-1</EndMinute>
        <EndMonth type="int">-1</EndMonth>
        <EndYear type="int">-1</EndYear>
      </Rule>
    </Rules>
  </User>
  <!---->
  <User name="test" type="Machine">
    <Enabled type="bool">true</Enabled>
    <Email type="string">noreply@sertainty.com</Email>
    <Expiration type="date">2120-02-03T18:00:00</Expiration>
    <FormalName type="string">test</FormalName>
    <Reality type="string"></Reality>
    <Privileges type="string">Read,Write,Owner</Privileges>
    <!---->
    <Private>
      <Workflow type="bool">false</Workflow>
      <Masking type="string">0</Masking>
```

```
<!---->
<HomeConfiguration>
  <Configuration>
    <Id type="int">1154337526</Id>
    <Name type="string">BozemanMTMMS-MACMT</Name>
    <Enabled type="bool">true</Enabled>
    <!---->
    <Device>
      <Id type="int">159995298</Id>
      <Name type="string">MMS-MACMT</Name>
    </Device>
    <!---->
    <Location>
      <Id type="int">3178502574</Id>
      <Name type="string">BozemanMT</Name>
      <Address type="string">4850 River Rd</Address>
      <City type="string">Bozeman</City>
      <Country type="string">US</Country>
      <InvalidLatitude type="string">0.000</InvalidLatitude>
      <InvalidLongitude type="string">0.000</InvalidLongitude>
      <InvalidRange type="string">0.000</InvalidRange>
      <Latitude type="string">45.73</Latitude>
      <Longitude type="string">-111.23</Longitude>
      <Range type="string">0.000</Range>
      <ScoreAddress type="string">5</ScoreAddress>
      <ScoreCity type="string">5</ScoreCity>
      <ScoreCountry type="string">5</ScoreCountry>
      <ScoreState type="string">5</ScoreState>
      <ScoreZipcode type="string">5</ScoreZipcode>
      <State type="string">MT</State>
      <TimeDiff type="string">33</TimeDiff>
      <Timestamp type="string">1601495073589</Timestamp>
      <Zipcode type="string">59718</Zipcode>
    </Location>
    <!---->
    <Network>
      <Id type="int">0</Id>
      <Name type="string"></Name>
      <InvalidIp type="string"></InvalidIp>
      <IpAddress type="string">69.163.84.195/192.168.1.14</IpAddress>
      <ScoreIP type="string">0</ScoreIP>
    </Network>
  </Configuration>
</HomeConfiguration>
<Rules>
  <Rule name="UserAdvanced">
    <MaximumTime type="int">60</MaximumTime>
    <MaximumTotalTime type="int">60</MaximumTotalTime>
    <MinimumTime type="int">0</MinimumTime>
    <MinimumTotalTime type="int">0</MinimumTotalTime>
  </Rule>
  <!---->
  <Rule name="UserBasic">
    <IgnoreCase type="bool">true</IgnoreCase>
    <IgnoreChars type="string"></IgnoreChars>
    <MinimumPrompts type="int">3</MinimumPrompts>
  </Rule>
  <!---->
  <Rule name="UserPanic">
    <Panic type="string"></Panic>
    <PanicEmail type="string"></PanicEmail>
    <PanicSMS type="string"></PanicSMS>
  </Rule>
  <!---->
  <Rule name="UserRecovery">
    <MaximumFailures type="int">0</MaximumFailures>
    <MinimumCorrect type="int">6</MinimumCorrect>
  </Rule>
</Rules>
<!---->
<Challenges>
  <Challenge name="!*>O>&lt;V/YH?A/W&amp;E>[_GL>X&lt;/A>]/O^H:DXIR--4ORGCLXIG#.">
    <Enabled type="bool">true</Enabled>
    <Hashed type="bool">false</Hashed>
    <Prompt type="string">!*&gt;O&gt;&lt;V/YH?A/W&amp;E&gt;[_GL&gt;X&lt;/A&gt;]/O^H:DXIR--
4ORGCLXIG#.</Prompt>
    <Required type="bool">true</Required>
    <Response type="string">2K&amp;!?.T&amp;W.%G34D,O[_/O#-H[V^R5CT+.S]A,N8R?$NSQ/@80;</Response>
```

```
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="%_S.,H3;ZW:B$JY?02]&lt;88#A??KYF],8UF589>OZ&amp;_WE/4%7GG">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">%_S.,H3;ZW:B$JY?02]&lt;88#A??KYF],8UF589&gt;OZ&amp;_WE/4%7GG</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">G&gt;S#T8%DQ&amp;R:OEYE!PS05?8?EZ&amp;9E67R!9Z,R#W%-
W%DT:3&amp;&amp;O</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name=".+8A5SEZ#D]?]E5![4&amp;*4%88?*O/4LC*3@%S$MMBB.,VA%[%H_">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">.+8A5SEZ#D]?]E5![4&amp;*4%88?*O/4LC*3@%S$MMBB.,VA%[%H_</Prompt>
            <Required type="bool">true</Required>
            <Response
type="string">G/NLD%_$BW2RP&lt;;[W?X&gt;G04SZ%!9P_Q9V*9/8EL[K9I@+&lt;A9?X</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="5+D3%8@REZ703&amp;C,4.KXT6>8A;HMZ7H3X&lt;6I&amp;0QYIU[8RW-[G>">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">5+D3%8@REZ703&amp;C,4.KXT6&gt;8A;HMZ7H3X&lt;6I&amp;0QYIU[8RW-
[G&gt;</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">8G#C22WM&gt;7LY9H:.!-^DE/8V,:44E7&lt;5&amp;Z-
&gt;ST5.TT7&gt;G7OTXO</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="7ZPM]]Q4_STBH_KF0$GD+X%K6H*ENJ,?ZVN4_-^RX8TUI8?NQ7">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">7ZPM]]Q4_STBH_KF0$GD+X%K6H*ENJ,?ZVN4_-^RX8TUI8?NQ7</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">&amp;J]T[&gt;2LF@G;V2JR@]^CWZ;+I+G-;UN&lt;CE5&lt;*;!9$V7^LU-
5$O</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="99!9HT]4%[;-[.ZXF4.RN5W3GKSN^M%Y2D]Y;D9_5U,_W&lt;@*F3">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">99!9HT]4%[;-[.ZXF4.RN5W3GKSN^M%Y2D]Y;D9_5U,_W&lt;@*F3</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">H]UW-60-
3&amp;K]HN]WK*NEKQ,B&lt;&amp;.9LH[@!^#!6068?O4VDOI&lt;5_</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="BX]*PXP4&amp;:CCJ^6SKY^U7$8B,@/_%#XUIVS^T.G@%P.LA@>N+Q">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">BX]*PXP4&amp;:CCJ^6SKY^U7$8B,@/_%#XUIVS^T.G@%P.LA@&gt;N+Q</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">BBHX7N!#9.^Q5+B#+Y8$*?&lt;QHN0OBQQ+3$H]J**]KQ@.X@?Y32</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="DWOA]QT-2TS&amp;5%H&amp;LO@IO7.20W:O-_H4ZTFP/2FK#&amp;J?URS&amp;TF">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">DWOA]QT-2TS&amp;5%H&amp;LO@IO7.20W:O-
_H4ZTFP/2FK#&amp;J?URS&amp;TF</Prompt>
            <Required type="bool">true</Required>
            <Response
type="string">9Y7/2Z?;@DMR2LE7*&lt;@:_JFD&lt;&lt;G&amp;A@YG5*UU0UGA,XBET32A&gt;0</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="P,??]_$[XJ!5C-QU&lt;G/.8U4I]V]MV4O&amp;#?&amp;2DT_MZ8,IJ93+MP">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">P,??]_$[XJ!5C-QU&lt;G/.8U4I]V]MV4O&amp;#?&amp;2DT_MZ8,IJ93+MP</Prompt>
```

```
            <Required type="bool">true</Required>
            <Response type="string">IKCH%ET2:]/T?$]_TDBX5/$0#T,/Q&gt;RO_V4SA[VYVOHP.#R&gt;$0</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
          <!---->
          <Challenge name="_;C9*&lt;C@$O45[CT[C75B@WH$&amp;]TT[NLRP,3S7:I_@9L6+4:.9X">
            <Enabled type="bool">true</Enabled>
            <Hashed type="bool">false</Hashed>
            <Prompt type="string">_;C9*&lt;C@$O45[CT[C75B@WH$&amp;]TT[NLRP,3S7:I_@9L6+4:.9X</Prompt>
            <Required type="bool">true</Required>
            <Response type="string">2QDEMS4TCBWULYW24!3&amp;?_8,&gt;EH&amp;B-_JDK?Q8-H/]+-
EX76FG5</Response>
            <Softkb type="bool">false</Softkb>
          </Challenge>
        </Challenges>
      </Private>
      <!---->
      <Rules>
        <Rule name="UserConfigurations">
          <Configurations>
            <Configuration>
              <Id type="int">1154337526</Id>
              <Name type="string">BozemanMT-test-MMS-MACMT</Name>
              <Enabled type="bool">true</Enabled>
              <!---->
              <Device>
                <Id type="int">159995298</Id>
                <Name type="string">test-MMS-MACMT</Name>
                <Architecture type="string">x86_64</Architecture>
                <CpuModel type="string">Intel(R) Core(TM) i7-8850H CPU @ 2.60GHz</CpuModel>
                <CpuSN type="string"></CpuSN>
                <CpuVendor type="string">GenuineIntel</CpuVendor>
                <DeviceType type="string">Mobile Device</DeviceType>
                <MachineModel type="string">MacBookPro15,1</MachineModel>
                <MachineName type="string">MMS-MACMT</MachineName>
                <MachineSN type="string">C02XT04LJG5J</MachineSN>
                <MachineUUID type="string">BE8E4898-8539-5467-93E0-A6B230DEEA07</MachineUUID>
                <MachineVendor type="string">Apple</MachineVendor>
                <OsFileId type="string">f7ead5f7eb1f</OsFileId>
                <OsMachine type="string">x86_64</OsMachine>
                <OsName type="string">MacOSX</OsName>
                <OsType type="string">Mac OS X</OsType>
                <OsUserName type="string">michellesmith</OsUserName>
                <OsVersion type="string">10.15.7</OsVersion>
                <Ram type="string">16384</Ram>
                <TimeZone type="string">-360</TimeZone>
                <TotalMemory type="string">17179869184</TotalMemory>
                <Vendor type="string">Apple</Vendor>
              </Device>
              <!---->
              <Location>
                <Id type="int">3178502574</Id>
                <Name type="string">BozemanMT</Name>
                <:anonymous type="string"></:anonymous>
                <:anonymous type="string"></:anonymous>
                <Address type="string">3535 River Rd</Address>
                <City type="string">Bozeman</City>
                <Country type="string">US</Country>
                <InvalidLatitude type="string">0.000</InvalidLatitude>
                <InvalidLongitude type="string">0.000</InvalidLongitude>
                <InvalidRange type="string">0.000</InvalidRange>
                <Latitude type="string">45.73</Latitude>
                <Longitude type="string">-111.23</Longitude>
                <Range type="string">0.000</Range>
                <ScoreAddress type="string">5</ScoreAddress>
                <ScoreCity type="string">5</ScoreCity>
                <ScoreCountry type="string">5</ScoreCountry>
                <ScoreState type="string">5</ScoreState>
                <ScoreZipcode type="string">5</ScoreZipcode>
                <State type="string">MT</State>
                <TimeDiff type="string">33</TimeDiff>
                <Timestamp type="string">1601495073589</Timestamp>
                <Zipcode type="string">59719</Zipcode>
              </Location>
              <!---->
              <Network>
                <Id type="int">0</Id>
                <Name type="string"></Name>
```

```
                <InvalidIp type="string"></InvalidIp>
                <IpAddress type="string">69.163.84.195/192.168.1.14</IpAddress>
                <ScoreIP type="string">0</ScoreIP>
              </Network>
            </Configuration>
          </Configurations>
        </Rule>
        <!---->
        <Rule name="UserApprovals">
          <ExternalLength type="int">6</ExternalLength>
        </Rule>
        <!---->
        <Rule name="UserSchedule">
          <Enabled type="bool">false</Enabled>
          <DaySunday type="bool">true</DaySunday>
          <DayMonday type="bool">true</DayMonday>
          <DayTuesday type="bool">true</DayTuesday>
          <DayWednesday type="bool">true</DayWednesday>
          <DayThursday type="bool">true</DayThursday>
          <DayFriday type="bool">true</DayFriday>
          <DaySaturday type="bool">true</DaySaturday>
          <StartDay type="int">-1</StartDay>
          <StartHour type="int">-1</StartHour>
          <StartMinute type="int">-1</StartMinute>
          <StartMonth type="int">-1</StartMonth>
          <StartYear type="int">-1</StartYear>
          <EndDay type="int">-1</EndDay>
          <EndHour type="int">-1</EndHour>
          <EndMinute type="int">-1</EndMinute>
          <EndMonth type="int">-1</EndMonth>
          <EndYear type="int">-1</EndYear>
        </Rule>
      </Rules>
    </User>
  <User name="test" type="Machine">
      <Enabled type="bool">true</Enabled>
      <Email type="string">noreply@sertainty.com</Email>
      <Expiration type="date">2120-02-03T18:00:00</Expiration>
      <FormalName type="string">test23</FormalName>
      <Reality type="string"></Reality>
      <Privileges type="string">Read,Write</Privileges>
      <!---->
      <Private>...encoded-user-data...</Private>
      <!---->
      <Rules>
        <Rule name="UserConfigurations">
          <Configurations>
            <Configuration>
              <Id type="int">1156777526</Id>
              <Name type="string">SanDiegoCA-Test23-XXX-MACCA</Name>
              <Enabled type="bool">true</Enabled>
              <!---->
              <Device>
                <Id type="int">159995232</Id>
                <Name type="string"> Test23-XXX-MACCA</Name>
                <Architecture type="string">x86_64</Architecture>
                <CpuModel type="string">Intel(R) Core(TM) i7-8750H CPU @ 2.60GHz</CpuModel>
                <CpuSN type="string"></CpuSN>
                <CpuVendor type="string">GenuineIntel</CpuVendor>
                <DeviceType type="string">Mobile Device</DeviceType>
                <MachineModel type="string">MacBookPro15,1</MachineModel>
                <MachineName type="string">XXX-MACCA</MachineName>
                <MachineSN type="string">C02XT04WJG5J</MachineSN>
                <MachineUUID type="string">BE8E4898-8909-5467-93E0-A6B230DEEA07</MachineUUID>
                <MachineVendor type="string">Apple</MachineVendor>
                <OsFileId type="string">f7ead8f7eb1f</OsFileId>
                <OsMachine type="string">x86_64</OsMachine>
                <OsName type="string">MacOSX</OsName>
                <OsType type="string">Mac OS X</OsType>
                <OsUserName type="string">Test23</OsUserName>
                <OsVersion type="string">10.15.7</OsVersion>
                <Ram type="string">16384</Ram>
                <TimeZone type="string">-360</TimeZone>
                <TotalMemory type="string">17179869184</TotalMemory>
                <Vendor type="string">Apple</Vendor>
              </Device>
              <!---->
              <Location>
```

```
                <Id type="int">3178502574</Id>
                <Name type="string">BozemanMT</Name>
                <:anonymous type="string"></:anonymous>
                <:anonymous type="string"></:anonymous>
                <Address type="string">4850 River Rd</Address>
                <City type="string">Bozeman</City>
                <Country type="string">US</Country>
                <InvalidLatitude type="string">0.000</InvalidLatitude>
                <InvalidLongitude type="string">0.000</InvalidLongitude>
                <InvalidRange type="string">0.000</InvalidRange>
                <Latitude type="string">45.73</Latitude>
                <Longitude type="string">-111.23</Longitude>
                <Range type="string">0.000</Range>
                <ScoreAddress type="string">5</ScoreAddress>
                <ScoreCity type="string">5</ScoreCity>
                <ScoreCountry type="string">5</ScoreCountry>
                <ScoreState type="string">5</ScoreState>
                <ScoreZipcode type="string">5</ScoreZipcode>
                <State type="string">MT</State>
                <TimeDiff type="string">33</TimeDiff>
                <Timestamp type="string">1601495073589</Timestamp>
                <Zipcode type="string">59718</Zipcode>
              </Location>
              <!---->
              <Network>
                <Id type="int">0</Id>
                <Name type="string"></Name>
                <InvalidIp type="string"></InvalidIp>
                <IpAddress type="string">69.163.84.195/192.168.1.14</IpAddress>
                <ScoreIP type="string">0</ScoreIP>
              </Network>
            </Configuration>
          </Configurations>
        </Rule>
        <!---->
        <Rule name="UserApprovals">
          <ExternalLength type="int">6</ExternalLength>
        </Rule>
        <!---->
        <Rule name="UserSchedule">
          <Enabled type="bool">false</Enabled>
          <DaySunday type="bool">true</DaySunday>
          <DayMonday type="bool">true</DayMonday>
          <DayTuesday type="bool">true</DayTuesday>
          <DayWednesday type="bool">true</DayWednesday>
          <DayThursday type="bool">true</DayThursday>
          <DayFriday type="bool">true</DayFriday>
          <DaySaturday type="bool">true</DaySaturday>
          <StartDay type="int">-1</StartDay>
          <StartHour type="int">-1</StartHour>
          <StartMinute type="int">-1</StartMinute>
          <StartMonth type="int">-1</StartMonth>
          <StartYear type="int">-1</StartYear>
          <EndDay type="int">-1</EndDay>
          <EndHour type="int">-1</EndHour>
          <EndMinute type="int">-1</EndMinute>
          <EndMonth type="int">-1</EndMonth>
          <EndYear type="int">-1</EndYear>
        </Rule>
      </Rules>
    </User>
  </Users>
```


4.5 Populated Schedule Rule Block

This defined Schedule is permitting access to the UXP Object


```
<Rule name="Schedule">
  <Enabled type="bool">true</Enabled>
  <DaySunday type="bool">true</DaySunday>
  <DayMonday type="bool">true</DayMonday>
  <DayTuesday type="bool">true</DayTuesday>
  <DayWednesday type="bool">true</DayWednesday>
  <DayThursday type="bool">true</DayThursday>
```

```
    <DayFriday type="bool">true</DayFriday>
    <DaySaturday type="bool">true</DaySaturday>
    <StartDay type="int">15</StartDay>
    <StartHour type="int">0</StartHour>
    <StartMinute type="int">0</StartMinute>
    <StartMonth type="int">3</StartMonth>
    <StartYear type="int">2021</StartYear>
    <EndDay type="int">15</EndDay>
    <EndHour type="int">23</EndHour>
    <EndMinute type="int">59</EndMinute>
    <EndMonth type="int">3</EndMonth>
    <EndYear type="int">2021</EndYear>
  </Rule>
```