API Operation Models from PingFederate **/oaut/ClientSettings** API's documentation

Operation Models

ClientSettings - The client settings. **{**

clientMetadata (array[ClientMetadata]): The client metadata.

dynamicClientRegistration (DynamicClientRegistration): Dynamic client registration settings.

}

ClientMetadata - The client metadata. **{**

parameter (string): The metadata name.

description (string): The metadata description.

multiValued (boolean): If the field should allow multiple values.

}

DynamicClientRegistration - Dynamic client registration settings. **{**

initialAccessTokenScope (string): The initial access token to prevent unwanted client registrations.

restrictCommonScopes (boolean): Restrict common scopes.

restrictedCommonScopes (array[string]): The common scopes to restrict.

allowedExclusiveScopes (array[string]): The exclusive scopes to allow.

requestPolicyRef (ResourceLink): The CIBA request policy.

enforceReplayPrevention (boolean): Enforce replay prevention.

requireSignedRequests (boolean): Require signed requests.

defaultAccessTokenManagerRef (ResourceLink): The default access token manager for this client.

restrictToDefaultAccessTokenManager (boolean): Determines whether the client is restricted to using only its default access token manager. The default is false.

persistentGrantExpirationType (PersistentGrantLifetimeType) = ['INDEFINITE_EXPIRY' or 'SERVER_DEFAULT' or 'OVERRIDE_SERVER_DEFAULT']: Allows an administrator to override the Persistent Grant Lifetime set globally for the OAuth AS. Defaults to SERVER_DEFAULT.

persistentGrantExpirationTime (integer): The persistent grant expiration time.

persistentGrantExpirationTimeUnit (PersistentGrantLifetimeUnit) = ['MINUTES' or 'DAYS' or 'HOURS']: The persistent grant expiration time unit.

persistentGrantIdleTimeoutType (PersistentGrantLifetimeType) = ['INDEFINITE_EXPIRY' or 'SERVER_DEFAULT' or 'OVERRIDE_SERVER_DEFAULT']: Allows an administrator to override the Persistent Grant Idle Timeout set globally for the OAuth AS. Defaults to SERVER_DEFAULT.

persistentGrantIdleTimeout (integer): The persistent grant idle timeout.

persistentGrantIdleTimeoutTimeUnit (PersistentGrantLifetimeUnit) = ['MINUTES' or 'DAYS' or 'HOURS']: The persistent grant idle timeout time unit.

clientCertIssuerType (ClientCertificateIssuerType) = ['NONE' or 'TRUST_ANY' or 'CERTIFICATE']: Client TLS Certificate Issuer Type.

clientCertIssuerRef (ResourceLink): Client TLS Certificate Issuer DN.

refreshRolling (RefreshRollingType) = ['SERVER_DEFAULT' or 'DONT_ROLL' or 'ROLL']: Use ROLL or DONT_ROLL to override the Roll Refresh Token Values setting on the Authorization Server Settings. SERVER_DEFAULT will default to the Roll Refresh Token Values setting on the Authorization Server Setting screen. Defaults to SERVER_DEFAULT.

refreshTokenRollingIntervalType (RefreshTokenRollingIntervalType) = ['SERVER_DEFAULT' or 'OVERRIDE_SERVER_DEFAULT']: Use OVERRIDE_SERVER_DEFAULT to override the Refresh Token Rolling Interval value on the Authorization Server Settings. SERVER_DEFAULT will default to the Refresh Token Rolling Interval value on the Authorization Server Setting. Defaults to SERVER_DEFAULT.

refreshTokenRollingInterval (integer): The minimum interval to roll refresh tokens, in hours. This value will override the Refresh Token Rolling Interval Value on the Authorization Server Settings.

oidcPolicy (ClientRegistrationOIDCPolicy): Open ID Connect Policy settings. This is included in the message only when OIDC is enabled.

policyRefs (array[ResourceLink]): The client registration policies.

deviceFlowSettingType (DeviceFlowSettingType) = ['SERVER_DEFAULT' or 'OVERRIDE_SERVER_DEFAULT']: Allows an administrator to override the Device Authorization Settings set globally for the OAuth AS. Defaults to SERVER_DEFAULT.

userAuthorizationUrlOverride (string): The URL is used as 'verification_url' and 'verification_url_complete' values in a Device Authorization request.

pendingAuthorizationTimeoutOverride (integer): The 'device_code' and 'user_code' timeout, in seconds.

devicePollingIntervalOverride (integer): The amount of time client should wait between polling requests, in seconds.

bypassActivationCodeConfirmationOverride (boolean): Indicates if the Activation Code Confirmation page should be bypassed if 'verification_url_complete' is used by the end user to authorize a device.

requireProofKeyForCodeExchange (boolean): Determines whether Proof Key for Code Exchange (PKCE) is required for the dynamically created client.

cibaPollingInterval (integer): The minimum amount of time in seconds that the Client must wait between polling requests to the token endpoint. The default is 3 seconds.

cibaRequireSignedRequests (boolean): Determines whether CIBA signed requests are required for this client.

tokenExchangeProcessorPolicyRef (ResourceLink): The Token Exchange Processor policy.

rotateClientSecret (boolean): Rotate registration access token on dynamic client management requests.

rotateRegistrationAccessToken (boolean): Rotate client secret on dynamic client management requests.

allowClientDelete (boolean): Allow client deletion from dynamic client management.

disableRegistrationAccessTokens (boolean): Disable registration access tokens. Local standards may mandate different registration access token requirements. If applicable, implement custom validation and enforcement rules using the DynamicClientRegistrationPlugin interface from the PingFederate SDK, configure the client registration policies (policyRefs), and set this property (disableRegistrationAccessTokens) to true. CAUTION: When the disableRegistrationAccessTokens property is set to true, all clients, not just the ones created using the Dynamic Client Registration protocol, are vulnerable to unrestricted retrievals, updates (including modifications to the client authentication scheme and redirect URIs), and deletes at the /as/clients.oauth2 endpoint unless one or more client registration policies are in place to protect against unauthorized attempts.

}
ResourceLink - A reference to a resource. **{**

id * (string): The ID of the resource.

location (string): A read-only URL that references the resource. If the resource is not currently URL-accessible, this property will be null.

}
ClientRegistrationOIDCPolicy - Client Registration Open ID Connect Policy settings. **{**

idTokenSigningAlgorithm (SigningAlgorithm) = ['NONE' or 'HS256' or 'HS384' or 'HS512' or 'RS256' or 'RS384' or 'RS512' or 'ES256' or 'ES384' or 'ES512' or 'PS256' or 'PS384' or 'PS512']: The JSON Web Signature [JWS] algorithm required for the ID Token.
NONE - No signing algorithm
HS256 - HMAC using SHA-256
HS384 - HMAC using SHA-384
HS512 - HMAC using SHA-512
RS256 - RSA using SHA-256
RS384 - RSA using SHA-384
RS512 - RSA using SHA-512
ES256 - ECDSA using P256 Curve and SHA-256
ES384 - ECDSA using P384 Curve and SHA-384
ES512 - ECDSA using P521 Curve and SHA-512
PS256 - RSASSA-PSS using SHA-256 and MGF1 padding with SHA-256
PS384 - RSASSA-PSS using SHA-384 and MGF1 padding with SHA-384
PS512 - RSASSA-PSS using SHA-512 and MGF1 padding with SHA-512
A null value will represent the default algorithm which is RS256.
RSASSA-PSS is only supported with SafeNet Luna, Thales nCipher or Java 11

idTokenEncryptionAlgorithm (EncryptionAlgorithm) = ['DIR' or 'A128KW' or 'A192KW' or 'A256KW' or 'A128GCMKW' or 'A192GCMKW' or 'A256GCMKW' or 'ECDH_ES' or 'ECDH_ES_A128KW' or 'ECDH_ES_A192KW' or 'ECDH_ES_A256KW' or 'RSA_OAEP']: The JSON Web Encryption [JWE] encryption algorithm used to encrypt the content encryption key for the ID Token.
DIR - Direct Encryption with symmetric key
A128KW - AES-128 Key Wrap
A192KW - AES-192 Key Wrap

A256KW - AES-256 Key Wrap
A128GCMKW - AES-GCM-128 key encryption
A192GCMKW - AES-GCM-192 key encryption
A256GCMKW - AES-GCM-256 key encryption
ECDH_ES - ECDH-ES
ECDH_ES_A128KW - ECDH-ES with AES-128 Key Wrap
ECDH_ES_A192KW - ECDH-ES with AES-192 Key Wrap
ECDH_ES_A256KW - ECDH-ES with AES-256 Key Wrap
RSA_OAEP - RSAES OAEP

idTokenContentEncryptionAlgorithm (ContentEncryptionAlgorithm)
= ['AES_128_CBC_HMAC_SHA_256' or 'AES_192_CBC_HMAC_SHA_384' or
'AES_256_CBC_HMAC_SHA_512' or 'AES_128_GCM' or 'AES_192_GCM' or 'AES_256_GCM']: The JSON Web Encryption [JWE] content encryption algorithm for the ID Token.
AES_128_CBC_HMAC_SHA_256 - Composite AES-CBC-128 HMAC-SHA-256
AES_192_CBC_HMAC_SHA_384 - Composite AES-CBC-192 HMAC-SHA-384
AES_256_CBC_HMAC_SHA_512 - Composite AES-CBC-256 HMAC-SHA-512
AES-GCM-128 - AES_128_GCM
AES_192_GCM - AES-GCM-192
AES_256_GCM - AES-GCM-256

policyGroup (ResourceLink): The Open ID Connect policy. A null value will represent the default policy group.

}