Links to Other API pages: Cisco Unity Connection APIs

CUPI Guide Contents
API Overview Index of All CUPI Documentation

Contents

About Authentication Rules

This section contains information on how to create, list, modify, and delete Authentication Rules. In Cisco Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. You use authentication rules to secure how users access Connection by phone, and how users access Cisco Unity Connection Administration and the Cisco Personal Communications Assistant (PCA).

For example, an authentication rule determines:

- The number of failed sign-in attempts that are allowed before an account is locked
- The number of minutes an account remains locked before it is reset
- Whether a locked account must be unlocked manually by an administrator
- The minimum length allowed for passwords and PINs
- The number of days before a password or PIN expires

Listing Authentication Rules

Example 1

The following is an example of the GET request that lists the Authentication Rules:

```
https://<connection_server>/vmrest/authenticationrules
```

The following is an example of the response from the above *GET* request and the actual response will depend upon the information given by you:

```
<AuthenticationRules total="2">
 <AuthenticationRule>
   <URI>/vmrest/authenticationrules/db3999dc-7afc-4a1e-be64-c5647c7f2226</URI>
   <ObjectId>db3999dc-7afc-4a1e-be64-c5647c7f2226</ObjectId>
   <HackResetTime>30</HackResetTime>
   <LocationObjectId>be27976c-6e6e-419f-853d-b3764881dfb0</LocationObjectId>
   <LocationURI>/vmrest/locations/connectionlocations/be27976c-6e6e-419f-853d-b3764881dfb0</Locati
   <LockoutDuration>30</LockoutDuration>
   <MaxDays>120</MaxDays>
   <MaxHacks>7</MaxHacks>
   <MinLength>8</MinLength>
   <PrevCredCount>5</PrevCredCount>
   <TrivialCredChecking>true</TrivialCredChecking>
   <DisplayName>Papa Recommended Web Application Authentication Rule</DisplayName>
   <MinDuration>1440</MinDuration>
   <ExpiryWarningDays>15</ExpiryWarningDays>
 </AuthenticationRule>
 <AuthenticationRule>
   <URI>/vmrest/authenticationrules/df3611a3-d372-4a38-a7a4-7d4aba4febd2</URI>
   <ObjectId>df3611a3-d372-4a38-a7a4-7d4aba4febd2</ObjectId>
   <HackResetTime>30</HackResetTime>
   <LocationObjectId>be27976c-6e6e-419f-853d-b3764881dfb0</LocationObjectId>
   <LocationURI>/vmrest/locations/connectionlocations/be27976c-6e6e-419f-853d-b3764881dfb0</Locati
   <LockoutDuration>30</LockoutDuration>
   <MaxDays>180</MaxDays>
   <MaxHacks>3</MaxHacks>
   <MinLength>6</MinLength>
   <PrevCredCount>5</PrevCredCount>
   <TrivialCredChecking>true</TrivialCredChecking>
   <DisplayName>Recommended Voice Mail Authentication Rule</DisplayName>
   <MinDuration>1440</MinDuration>
   <ExpiryWarningDays>15</ExpiryWarningDays>
 </AuthenticationRule>
 <AuthenticationRule>
   <URI>/vmrest/authenticationrules/5780fb3f-8f70-4d3d-9c18-2832f9d11642</URI>
   <ObjectId>5780fb3f-8f70-4d3d-9c18-2832f9d11642</ObjectId>
   <HackResetTime>30</HackResetTime>
   <LocationObjectId>be27976c-6e6e-419f-853d-b3764881dfb0</LocationObjectId>
   <LocationURI>/vmrest/locations/connectionlocations/be27976c-6e6e-419f-853d-b3764881dfb0</Locati
   <LockoutDuration>30</LockoutDuration>
   <MaxDays>180</MaxDays>
   <MaxHacks>3</MaxHacks>
   <MinLength>8</MinLength>
   <PrevCredCount>12</PrevCredCount>
   <TrivialCredChecking>true</TrivialCredChecking>
   <DisplayName>test</DisplayName>
   <MinDuration>0</MinDuration>
   <ExpiryWarningDays>15</ExpiryWarningDays>
 </AuthenticationRule>
 <AuthenticationRule>
   <URI>/vmrest/authenticationrules/ac80ee1d-0f09-42d0-ae7c-adb56a82b340</URI>
   <ObjectId>ac80ee1d-0f09-42d0-ae7c-adb56a82b340</ObjectId>
   <HackResetTime>30</HackResetTime>
   <LocationObjectId>be27976c-6e6e-419f-853d-b3764881dfb0</LocationObjectId>
   <LocationURI>/vmrest/locations/connectionlocations/be27976c-6e6e-419f-853d-b3764881dfb0</Locati
   <LockoutDuration>30</LockoutDuration>
   <MaxDays>180</MaxDays>
   <MaxHacks>3</MaxHacks>
   <MinLength>8</MinLength>
   <PrevCredCount>12</PrevCredCount>
   <TrivialCredChecking>true</TrivialCredChecking>
   <DisplayName>Papa Recommended Web Application Authentication Rule Paapas</DisplayName>
   <MinDuration>1440</MinDuration>
   <ExpiryWarningDays>15</ExpiryWarningDays>
```

```
 </AuthenticationRule>
</AuthenticationRules>

 Response code: 200
```

Example 2

The following is an example of the GET request that lists a specified Authentication Rule as represented by <objectId>:

```
https://<connection_server>/vmrest/authenticationrules/<objectId>
```

The following is an example of the response from the above *GET* request and the actual response will depend upon the information given by you:

```
<AuthenticationRule>
 <URI>/vmrest/authenticationrules/db3999dc-7afc-4a1e-be64-c5647c7f2226</URI>
 <ObjectId>db3999dc-7afc-4a1e-be64-c5647c7f2226</ObjectId>
 <HackResetTime>30</HackResetTime>
 <LocationObjectId>be27976c-6e6e-419f-853d-b3764881dfb0</LocationObjectId>
 <LocationURI>/vmrest/locations/connectionlocations/be27976c-6e6e-419f-853d-b3764881dfb0</Location
 <LockoutDuration>30</LockoutDuration>
 <MaxDays>120</MaxDays>
 <MaxHacks>7</MaxHacks>
 <MinLength>8</MinLength>
 <PrevCredCount>5</PrevCredCount>
 <TrivialCredChecking>true</TrivialCredChecking>
 <DisplayName>Papa Recommended Web Application Authentication Rule</DisplayName>
 <MinDuration>1440</MinDuration>
 <ExpiryWarningDays>15</ExpiryWarningDays>
</AuthenticationRule>

 Response code: 200
```

Adding a new Authentication Rule

The following is an example of the POST request that lists the Authentication Rules:

```
 https://<connection_server>/vmrest/authenticationrules
```

The following is an example of the response from the above *POST* request and the actual response will depend upon the information given by you:

```
<AuthenticationRule>
<DisplayName>New Authentication Rule</DisplayName>
<HackResetTime>30</HackResetTime>
 <LockoutDuration>30</LockoutDuration>
 <MaxDays>120</MaxDays>
 <MaxHacks>7</MaxHacks>
 <MinLength>8</MinLength>
 <PrevCredCount>5</PrevCredCount>
 <TrivialCredChecking>true</TrivialCredChecking>
 <MinDuration>1440</MinDuration>
 <ExpiryWarningDays>15</ExpiryWarningDays>
</AuthenticationRule>

 Response code: 201
```

Modifying Authentication Rules

The following is an example of the PUT request that modifies the Authentication Rule:

```
 https://<connection_server>/vmrest/ authenticationrules/<objectId>
```

The actual response will depend upon the information given by you.

```
<AuthenticationRule> <AuthenticationRule>
<HackResetTime>60</HackResetTime>
 <LockoutDuration>60</LockoutDuration>
 <MaxDays>120</MaxDays>
 <MaxHacks>7</MaxHacks>
 <MinLength>8</MinLength>
 <PrevCredCount>5</PrevCredCount>
 <TrivialCredChecking>true</TrivialCredChecking>
 <MinDuration>1440</MinDuration>
 <ExpiryWarningDays>15</ExpiryWarningDays>
</AuthenticationRule>
<HackResetTime>60</HackResetTime>
 <LockoutDuration>60</LockoutDuration>
 <MaxDays>120</MaxDays>
 <MaxHacks>7</MaxHacks>
 <MinLength>8</MinLength>
 <PrevCredCount>5</PrevCredCount>
 <TrivialCredChecking>true</TrivialCredChecking>
 <MinDuration>1440</MinDuration>
 <ExpiryWarningDays>15</ExpiryWarningDays>
</AuthenticationRule>

 Response code: 204
```

Deleting Authentication Rules

The following is an example of the DELETE request that deletes a Authentication Rule as represented by <objectId>:

```
 https://<connection_server>/vmrest/authenticationrules/<objectId>
```

The output for this request returns the successful response code.

```
 Response Code: 204
```

Explanation of Data Fields

The following chart lists all of the data fields available on Authentication Rules.

Field Name	Writable?	DB Values	Explanation / Comments
HackResetTime	Read/Write	1-120	Reset Every Failed Sign-In Attempts. Default: 30
LockoutDuration	Read/Write	0-1440	LockoutDuration. Default: 30
MaxDays	Read/Write	0-3653	Credential Expires After. Default=180

MaxHacks	Read/Write	0-100	Failed Sign-In. Default=3
MinLength	Read/Write	1-64	Minimum credential length. Default: 8
PrevCredCount	Read/Write	0-25	Stored Number of Previous Credentials. Default=12
TrivialCredChecking	Read/Write	true/false	Check for Trivial Passwords. Default=false
DisplayName	Read/Write	1-64	Friendly name for the Authentication Rule.
MinDuration	Read/Write	0-129600	Minimum Duration between Credential Changes
ExpiryWarningDays	Read/Write		Expiration Warning Days. Default=15