Managing Client Access Rules

Applies to: *Exchange Online Dedicated - Legacy 2013 & vNext Releases*

Topic Last Modified: *13-Oct-2015*

Client Access Rules help you to control access to your Exchange Online organization based upon the properties of the client or the access request type of the client. The rules are used to block the ability of a client to use a particular protocol, application, service, or resource based upon username, source IP address or range, the authentication type, or a recipient attribute. Examples include the following:

- Blocking Exchange ActiveSync (EAS) clients
- Blocking access to Outlook Web Access (OWA)
- Blocking access to Exchange Web Service (EWS)
- Blocking access to an Offline Address Book (OAB)
- Preventing client access using federated authentication
- Preventing client access to PowerShell
- Blocking access for users of a particular country or region to the Exchange Admin Center (EAC)

Client access rules are like transport rules for client connections to your Exchange Online environment. Conditions and exceptions are applied to each client connection attempt based upon the properties of the user or the properties of the client connection. Actions that you define and associate with specific conditions and exceptions are executed when a match occurs. Each rule also is assigned a priority number to dictate the sequence to evaluate each rule.

Note:

- Client Access Rules is a self-service administration feature and only available in the ANSI 2013 and vNext releases of the Dedicated and ITAR-support plans of Exchange Online.

Important:

- When blocking the use of a specific protocol, note that other applications that rely on the same protocol also may be impacted. Blocking the use of Exchange Web Services (EWS) in a vNext environment, for example, will impact the ability to use the Outlook Mail REST API.

Internal Messaging Traffic

Messaging traffic between your internal client systems and Exchange Online is always allowed due to the presence of several default client access rules Microsoft has created for your environment. These default rules (a) prevent your custom rules from blocking administrative access from your internal corporate network and (b) prevent monitoring and system management functions provided by Microsoft from being impacted. When viewing client access rules, the default rules will appear as "`Microsoft Datacenter Reserved`" (or similar wording) in the **Name** field of the rule list.

Note:

- The presence of the default rules allows you to create custom rules without the need to specify any IP ranges since all custom rules apply to Internet access. An example is the following to block Exchange ActiveSync access from the Internet:

```
New-ClientAccessRule -Name "Block ActiveSync from Internet" -Action DenyAccess -
AnyOfProtocols ExchangeActiveSync
```

- With the vNext offering of Exchange Online Dedicated, default client access rules created by Microsoft do not exist which means traffic from your internal network is not automatically allowed through the Client Access Rules feature. If you want to ensure that your internal clients can always access Exchange Online, you must create rules that allow access from your outbound Secure Network Address Translation (SNAT) IP addresses.

Rule Evaluation

If multiple rules exist, the rule-evaluation engine will evaluate the incoming Exchange access request by applying each rule in sequence. The rules are applied in the order they were created (default priority ranking) or by the priority value manually set on each rule. As soon as a match is found, the engine will stop evaluating rules and the access request is granted or denied based upon the conditions within the matching rule. The following illustrates the execution of rule evaluation:

1. Your environment has only one client access rule blocking all Outlook Web App (OWA) traffic from the Internet:

```
Name                          Priority        Enabled       DatacenterAdminsOnly
----                          --------        -------       --------------------
Block OWA from the Internet   1               True          False
```

2. To open up access for certain IP ranges, you create a rule to explicitly allow that IP range:

```
New-ClientAccessRule -Name "Allow OWA for IPs" -Action AllowAccess -AnyOfProtocols
OutlookWebAccess -AnyOfClientIPAddressesOrRanges 192.168.10.1/24
```

3. You now have the following two rules (notice the new rule has been automatically assigned an incremental priority of 2):

```
Name                              Priority            Enabled       DatacenterAdminsOnly
----                              --------            -------       --------------------
Block OWA from the Internet       1                   True          False
Allow OWA for IPs                 2                   True          False
```

The priority ranking of the rules will not achieve the desired result since all OWA requests initiated from the Internet will be blocked by the first rule including traffic from 192.168.10.1/24 IP range; successful execution of the Priority 1 rule will terminate the evaluation engine.

4. The recommended approach is to modify the existing Priority 1 rule and use the "except" parameter:

```
Set-ClientAccessRule "Block OWA from the Internet" -ExceptAnyOfClientIPAddressesOrRanges
192.168.10.1/24
```

Required Management Permissions

You need to be assigned the required Role Based Access Control (RBAC) permissions for your Exchange Online environment before you can run the Client Access Rules cmdlets. Although all parameters for the cmdlets are listed in the topics, you may not have access to some of the parameters if they're not included in the permissions assigned to you.

ANSI & ITAR-support Permissions

The Client Access Rules cmdlets for an ANSI or ITAR-support environment are included within the **SSA_Organization Client Access** role which is associated with the **SSA-Organization Configuration** role group. The Self-Service Administration Guide of the *Exchange Online Dedicated Release Collateral* library describes the RBAC model for the legacy platform releases.

vNext & Enhanced Permissions

The vNext and Enhanced releases of Exchange Online are based upon the multi-tenant RBAC model of Exchange Online (see Permissions in the Exchange Online service description). The Client Access Rules cmdlets for a vNext or Enhanced environment are included within the Organization Client Access role which is associated with the Organization Management role group.

Cmdlet Set

Windows PowerShell cmdlets are available to create, modify, delete, view, and test client access rules. The cmdlet set provides a self-service capability to you and administrators within your organization.

Create a Client Access Rule

```
New-ClientAccessRule -Name "Block ActiveSync" -Action DenyAccess -AnyOfProtocols
ExchangeActiveSync -ExceptAnyOfClientIPAddressesOrRanges 192.168.10.1/24
```

For additional parameters, setting details, and examples of cmdlet usage, see New-ClientAccessRule.

Modify an existing Client Access Rule

```
Set-ClientAccessRule "Allow IMAP4" -AnyOfClientIPAddressesOrRanges
@{Add=”172.17.17.27/16”}
```

For additional parameters, setting details, and examples of cmdlet usage, see Set-ClientAccessRule.

Delete an existing Client Access Rule

```
Remove-ClientAccessRule "Block Client Connections from 192.168.1.0/24"
```

For additional parameters, setting details, and examples of cmdlet usage, see Remove-ClientAccessRule.

View the settings of a Client Access Rule

```
Get-ClientAccessRule "Block Client Connections from 192.168.1.0/24" | Format-List
```

For additional parameters, setting details, and examples of cmdlet usage, see Get-ClientAccessRule.

Test a Client Access Rule

```
Test-ClientAccessRule -AuthenticationType BasicAuthentication -Protocol OutlookWebApp -
RemoteAddress 172.17.17.26 -RemotePort 443 -User julia@contoso.com
```

For additional parameters, setting details, and examples of cmdlet usage, see Test-ClientAccessRule.