Successfactors RCM Outlook Integration Troubleshooting Guide v1.0

This document can be used to ensure that Exchange Web Service EWS is correctly configured at Customers Microsoft Exchange. These steps mostly remain same for On-Premise and On-Demand exchange installations.

Pre-Condition checklist:

1]
What is the version of Exchange server used?
Successfactors currently support 2007 On-premise, 2010 On-premise, 2013 On-premise, Office 365 On-Demand.

2]
Please ensure that requests from Recruiting Customer Facing App server (hosted inside SuccessFactors/SAP data center) to Customers Microsoft Exchange Web Services are not restricted by customer's network firewall.

a. Ensure port http, https are open– generally these are 80 & 443

3]
Please ensure AutoDiscover Service is running and published outside of customer's network firewall, in public-internet domain.

4]
Please ensure that inside of Client Access Server role(CAS), paths to EWS[*/ews/**] and AutoDiscover[*/AutoDiscover/**] are configured in a way so that they are accessible to public-internet. Access to these URL paths should not be restricted by security software like Microsoft ISA, Microsoft PMG etc.

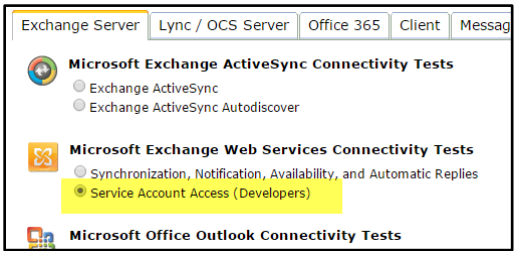
5]
Exchange administrators can control client application access to EWS in Exchange. Following Exchange Management Shell cmdlets can be used to configure EWS access controls. Use the Get-OrganizationConfig cmdlet to make sure that EWS is enabled on the server, and the Get-CASMailbox cmdlet to make sure that EWS is enabled for the Service Account user's mailbox. Also check both cmdlet responses for an EWS allow or block list, and make sure that your application isn't blocked from using EWS.

Get-CASMailbox - https://technet.microsoft.com/en-us/library/bb124754.aspx
Set-CASMailbox - https://technet.microsoft.com/en-us/library/bb125264.aspx
Get-OrganizationConfig - https://technet.microsoft.com/en-us/library/aa997571.aspx
Set-OrganizationConfig - https://technet.microsoft.com/en-us/library/aa997443.aspx
Sample usage:
Get-CASMailbox serviceaccount@customerdomain.com | Format-List Ews*

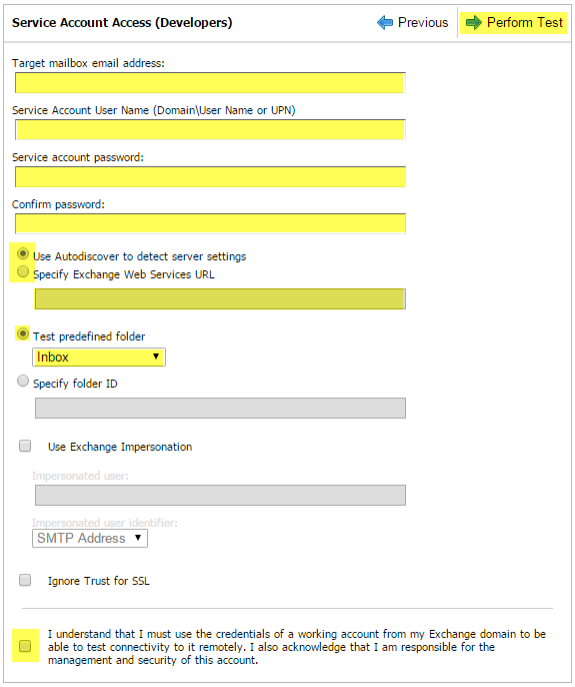
Get-OrganizationConfig | Format-List EwsApplicationAccessPolicy,Ews*List

Troubleshooting:

1]
Most popular way to start troubleshooting is using the online tool provided by Microsoft at https://testconnectivity.microsoft.com
Click on Microsoft Exchange Web Services Connectivity Tests -> Service Account Access (Developers)



You can perform test for both Exchange URL & Autodiscover. Provide the required parameters and click “Perform Test”



2]
Analysis of result will point to the root cause of the issue.

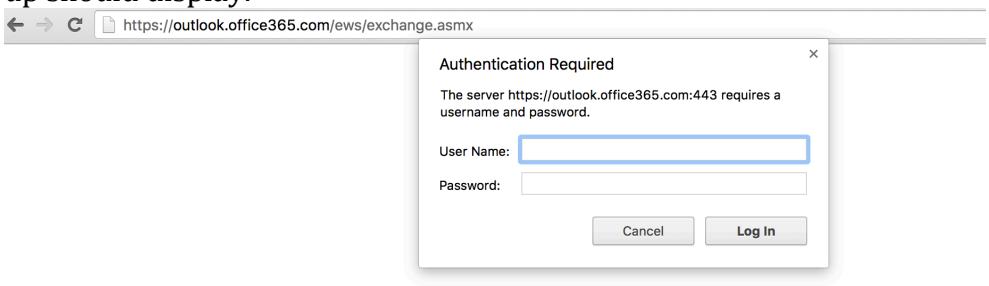
3]
If you see an error stack trace. Get access to customers Exchange server. The logging functionality provided by Internet Information Services (IIS) on the Client Access

servers can provide more information about failures. However, keep in mind that IIS logs will only be helpful if you are receiving an HTTP error.

4]
To validate if EWS service is correctly published, try accessing customer's exchange EWS URL from a browser by replacing the "email.customer.com" in the following:

https://email.customer.com/ews/exchange.asmx

Please ensure you are outside the customer's internal network. Authentication pop-up should display.



If you do not see this Authentication pop-up, chances are EWS service is not accessible outside customer's network.

5]
Verify with the Exchange Administrator that throttling policies will not affect EWS. More information on EWS throttling can be found at
https://msdn.microsoft.com/en-us/library/office/jj945066(v=exchg.150).aspx

6]
Some customers use a "self-signed" certificate or an internal Certificate Authority (CA) rather than a public CA, for services like Exchange that may be considered internal. If SuccessFactors/SAP is not able to validate the certificate any https-connection request will fail until the certificate has been installed into the SucessFactors keystore.
This integration requires that a trusted connection already exists between servers. Using a certificate from a Public Certificate Authority has the advantage that it gives automatic "trust" of that certificate.
However if you see an error relating to Certificates while running the tests at https://testconnectivity.microsoft.com then this might need further engineering assistance. Please contact Customer Support for a JIRA.