# **Reverse Logistics Onboarding Documentation**

Overview

In order to use Microsoft's Automated Reverse Logistics Program, organizations are required to sign up for an account with SysDev

* Purchase an Authenticode signing certificate
* Install the certificate on all machines that will be used to submit requests
* Assign an administrator(s) to manage the program
* Associate each individual Microsoft Account/user to the company and grant them 'ReverseLogistics' claims on that account.

Registering a Group (called "Company" on the Hardware Portal)

**Note:** Your company may already have a company account with the Microsoft Hardware portal. You will need to find the administrator of your company group on the Hardware Portal and add a reverse logistics manager as an additional administrator so it's easier to approve users' reverse logistics requests.

The reverse logistics team at the partner company needs to designate an administrator who will be in charge of adding and removing members in their group.

The first step is for this designated admin to register the company Reverse Logistics team.

Here's how to get registered:

1. [Get a code signing certificate](https://msdn.microsoft.com/library/windows/hardware/hh801887)
   * **Note**: In order to use RL, you \*must\* purchase a standard class 3 certificate, NOT a EV certificate.
   * Make sure you establish your company with the same name you purchase the certificate, and this is the name that will be exposed to users on email.
2. [Establish a company](https://msdn.microsoft.com/library/windows/hardware/br230795.aspx)

Make sure you save this certificate and that it is accessible. You will need to install it on multiple machines later in the Provisioning Workstations section. We recommend you save a copy of the certificate onto a thumbdrive, or something easily accessible.

Setting your Group Up to Use the Reverse Logistics Capability

You will need to email Microsoft's SysDev Support center and ask them to add the Reverse Logistics Capability to your users' list of roles [sysdev@microsoft.com](mailto:sysdev@microsoft.com).

Additional MSDN help documentation for generic role management for admins at <https://msdn.microsoft.com/en-us/library/windows/hardware/br230781.aspx>

Adding Users to the Group

Now that you have successfully created a RL group, you will need to add all requestors who need Reverse Logistics access to the group.

**Roles**

* The first person to create the group/company becomes an admin of the group.
* Subsequent users will be able to register their Microsoft Account with a particular group/company and request the roles he would like to have.
  + Note: Each user \*must\* select the Reverse Logistics role
* Admin gets a notification and will approve the request for those roles.

**Instructions:** [Add a user or migrate an account](https://msdn.microsoft.com/library/windows/hardware/br230782)

1. Have each user [sign in to the hardware dashboard](https://sysdev.microsoft.com/hardware/)
2. On the top right-hand corner of the dashboard, click **Register** to add yourself to your company and request the permissions you need from your company administrator.

**IMPORTANT:** Make sure each user selects the checkbox for **Reverse Logistics** under Additional Permissions Request

Administrator Responsibilities

Includes:

* Approving requests to join the group
* Approving authorizations requested, e.g. "Reverse Logistics"
* Revoking authorizations, e.g. when an employee leaves the company.

Setting up your Workstation for Reverse Logistics

Pre-requisites

* Partners must have a workstation that has browser access to the internet.
* This workstation must run Windows 7+
* Each RL submitter must have their own MSA; they should not share account credentials across multiple people.
* Note that only machines that have the certificate installed on it will be able to perform RL.

Process

1. Plug in the thumb drive which contains the certificate you purchased (if applicable).
2. Install the code signing certificate on each PC you want to submit RL requests from. To do so follow the below instructions:
   1. Open a Command Prompt window.
   2. Type mmc and press the ENTER key. Note that to view certificates in the local machine store, you must be in the Administrator role.
   3. On the File menu, click Add/Remove Snap In.
   4. Click Add.
   5. In the Add Standalone Snap-in dialog box, select Certificates.
   6. Click Add.
   7. In the Certificates snap-in dialog box, select Computer account and click Next.
   8. In the Select Computer dialog box, click Finish.
   9. In the Add Standalone Snap-in dialog box, click Close.
   10. On the Add/Remove Snap-in dialog box, click OK.
   11. In the Console Root window, click Certificates (Local Computer) to view the certificate stores for the computer.
   12. In the Actions pane, select 'More Actions' under Certificates, then All Tasks, and then Import:

Machine generated alternative text:
rtificates 
Request New Certificate. 
mpot... 
Advanced Operations 
Page 
All Tasks 
V iew 
New Window from Here 
New Taskpad View... 
Refresh 
Export List... 
Help 

1. Now, click Browse and find the certificate you purchased.
2. Click OK. The certificate should be installed in your Personals folder. If it is not, move it to that folder.

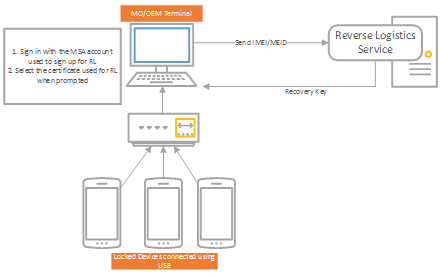
Authentication and Use

Now your RL team can create a client tool on the provisioned workstation to submit Reverse Logistics requests.

You will need to create a third party app with Microsoft Account (MSA), which will use a browser window to allow users to enter credentials via an MSA website to grant access to your tool to get the appropriate token to call the Reverse Logistics API. Follow this tutorial, using the "dds.reverse\_logistics" scope (instead of "wl.basic") to get the appropriate token:

<https://msdn.microsoft.com/en-us/library/hh826529.aspx>

Once your tool has the token, it can call the Reverse Logistics API with that token, your client certificate, and the target IMEI in order to retrieve the recovery key for the target device.



API Specification

#### Request

Reverse Logistics API endpoint:

POST [https://cs.dds.microsoft.com/Command/ExternalClientCert/AdministrativeUnprotect/{PartnerName}/{DeviceId}](https://cs.dds.microsoft.com/Command/ExternalClientCert/AdministrativeUnprotect/%7bPartnerName%7d/%7bDeviceId%7d)

{PartnerName} should be replaced with an end-user readable string that will be included in an email to the user whose Microsoft Account is protecting the phone.

{DeviceId} should be replaced with a string in one of the following formats (leaving the square brackets and replacing the text inside and including the curly brackets):

* ImeiOrMeid[{IMEI or MEID of the device}]
* Duid[{DUID of the device}]

Include the MSA user token in the “Authorization” header of the request.

The certificate provisioned with SysDev for your organization must be used as the client certificate for mutual HTTPS.

#### Response

If successful, the response will be JSON in the following format:

{

"UnprotectResult": "{UnprotectResult}"

"RecoveryKey": "{RecoveryKey}"

}

UnprotectResult will be a string value of the enum specified below:

/// <summary>

/// Result of the unprotect operation

/// </summary>

public enum UnprotectResult

{

/// <summary>

/// Device was not found in DDS

/// </summary>

DeviceNotFound,

/// <summary>

/// Device was already unprotected

/// </summary>

DeviceAlreadyUnprotected,

/// <summary>

/// Device has been unprotected

/// </summary>

DeviceUnprotected,

/// <summary>

/// IF we find more than 1 device, we don't currently have a way to resolve the conflict. So, we don't unprotect.

/// </summary>

MultipleDevicesFound,

}

Response codes:

* 200: Success.
* 400: The request is malformed
* 401: The request is unauthorized. Your organization may not be provisioned properly, the user may not be provisioned with the organization, or there may be a problem or mismatch with the client certificate or the MSA user token. The response may include text giving a reason for the authorization problem.
* 404: The API path or device specified was not found.
* 500: An unexpected error. If this persists, contact Microsoft for resolution of the issue.
* 503: Storage error. If this persists, contact Microsoft for resolution of the issue.