Remote Device Wipe via Microsoft Intune

Purpose

To define the standardized procedure for initiating a remote wipe of organizational devices through Microsoft Intune. This ensures data security and compliance in the event of a device loss, theft, separation, or decommissioning.

1. Confirm the device is enrolled in Intune and listed in the Intune Admin Center.
2. Validate that the device is actively checking in (last sync time within 24 hours).
3. Ensure proper incident ticket has been opened and documented.
4. Review assigner user account, device ownership type, and data sensitivity classification.
5. Go to <https://endpoint.microsoft.com/> and sing in using your Global Administrator or Intune Admin credentials.
6. Navigate to **Devices > All Devices** and search for and select the target device.
7. Match device information (device name, OS type, serial number, and assigned user) against inventory records in InvGate, device setup or asset tag information, and linked tickets.
8. Once verified, initiate remote wipe:
   1. Click on the device entry.
   2. Review device compliance status and las check-in time.
   3. In top action bar, click “Wipe”.
   4. Configure wipe options:

* **Retain enrollment state and user account**: Unchecked for full factory reset.
* **Wipe device, and continue to wipe even if device is offline**: Checked to enable auto-wipe once the device re-connects to the Internet).
  1. Confirm the action by selecting “Yes” when prompted.
  2. Update ticket with time of wipe initiation.

NOTE: This action is irreversible and removes all organizational and personal data from the device.

1. Monitor the device status in Intune:
   1. If successful, the device status will update to “Wipe pending” and then “Wipe complete”.
   2. If unsuccessful after 72 hours, document the failure and escalate.
   3. Update ticket with wipe status.
2. Mark the device as “Decommissioned”, “Retired”, or “Lost” in inventory system.
3. If applicable, file e-waste or device replacement per the Asset Management and Inventory Tracking SOP as well as the IT Procurement SOP.
4. Special Scenarios
   1. If the device is no longer checking in: Select “Wipe when next online” option and, if it has not connected within seven days flag in the ticket for re-evaluation.
   2. If device has sensitive data and wipe fails: Initiate credential reset, disable user sessions, and follow Devie Loss or Theft or Data Breaches SOPs if needed.
   3. If the user is active and cooperative: Notify them before initiating the wipe unless policy dictates otherwise (such as in an involuntary termination).