Geräteverwaltung & ZDM

Informationen zum Zentralen Desktopmanagement und zur Verwaltung von Dienstgeräten.

- Was ist ZDM und warum ist es wichtig an Universitäten?
- Warum unterstützt ITAU nur eine Hand voll unterschiedlicher Modelle für IT Hardware?
- Aktualisierung von ZENworks auf ZDM-Rechnern
- Neubereitstellung von ZDM-Geräten
- BitLocker-Recovery nach Lenovo-Firmware- oder BIOS-Update
- ZDM-Rechner für Präsentationen wach halten / automatische Bildschirmsperre

Was ist ZDM und warum ist es wichtig an Universitäten?

Zentrales Desktop Management (ZDM) ist die zentrale Verwaltung von Geräten wie Stand Pcs, Workstations oder Laptops, die von Studierenden, Lehrenden und Mitarbeitenden an Universitäten genutzt werden. ZDM ermöglicht es, die Sicherheit und Funktionalität der Geräte zu gewährleisten, die auf das universitäre Netzwerk und die Daten zugreifen.

ZDM ist wichtig an Universitäten, weil:

- Die Sicherheit der universitären Daten und Systeme vor unbefugtem Zugriff, Viren oder anderen Bedrohungen geschützt werden muss. ZDM erlaubt es, Sicherheitsrichtlinien und -einstellungen für alle mobilen Geräte festzulegen und auszurollen, wie zum Beispiel Passwortanforderungen, Verschlüsselung, VPN- und WLAN-Zugang, App-Berechtigungen oder Fernlöschung bei Verlust oder Diebstahl.
- Die Funktionalität der mobilen Geräte für die universitären Anwendungen optimiert werden muss. ZDM ermöglicht es, die Geräte mit den benötigten Apps, Daten, Updates und Patches zu versorgen, die Kompatibilität und Leistung zu überprüfen und die Nutzeraktivitäten zu überwachen.

ZDM bietet also viele Vorteile für Universitäten, indem es die Verwaltung, Sicherheit und Funktionalität der mobilen Geräte vereinfacht und verbessert. ZDM kann auch dazu beitragen, Kosten zu sparen, indem es den Supportaufwand reduziert, die Produktivität erhöht und die Compliance mit gesetzlichen Vorgaben sicherstellt.

Weitere Informationen finden Sie unter SCC: BSI-Schutz auf zentral administrierten Rechnern (Windows).

Warum unterstützt ITAU nur eine Hand voll unterschiedlicher Modelle für IT Hardware?

Sie haben Sie sich vielleicht schon einmal gefragt, warum die IT Abteilung nur bestimmte Modelle oder Marken unterstützt. Warum können Sie nicht einfach Ihr eigenes Gerät mitbringen oder das neueste Modell kaufen, das Ihnen gefällt?

Die Antwort liegt im Zentralen Desktop Management (ZDM). ZDM ist die zentrale Verwaltung von Geräten, die für die Sicherheit und Funktionalität der IT in der Universität sorgt. Mit einer ZDM-Lösung kann die IT Abteilung verschiedene Richtlinien und Einstellungen für die Geräte festlegen, wie zum Beispiel:

- Wie die Updates und Patches verteilt werden
- Wie Backups angelegt werden
- Wie oft ein Passwort geändert werden muss oder wie lang es sein muss
- Wie die Daten verschlüsselt oder gelöscht werden können, wenn das Gerät verloren geht oder gestohlen wird
- Wie der Zugang zum WLAN oder VPN konfiguriert wird
- Welche Apps installiert werden dürfen oder nicht

Diese Maßnahmen dienen dazu, die Daten und Systeme der Universität vor unbefugtem Zugriff, Viren oder anderen Bedrohungen zu schützen. Außerdem helfen sie dabei, die Produktivität und Effizienz der Mitarbeiter zu erhöhen, indem sie eine einheitliche und optimale Nutzung der Geräte ermöglichen.

Die Implementierung von ZDM ist jedoch nicht für jedes Gerät gleich einfach. Unterschiedliche Hersteller, Betriebssysteme und Modelle erfordern unterschiedliche Anpassungen und Kompatibilitätsprüfungen. Je mehr Geräte die IT-Abteilung unterstützen muss, desto mehr Aufwand und Kosten entstehen. Deshalb entscheiden sich viele Universitäten dafür, nur eine feste Anzahl unterschiedlicher Geräte zu unterstützen, die ihren Anforderungen am besten entsprechen.

Fazit: Die IT Abteilung unterstützt nur eine Hand voll unterschiedliche Geräte, weil sie damit das Zentrale Desktop Management einfacher und effektiver gestalten kann. Das kommt sowohl der Universität als auch den Mitarbeitern zugute.

Aktualisierung von ZENworks auf ZDM-Rechnern

Der **ZENworks-Agent** der zentral betreuten Windows-Computer (ZDM) muss in **regelmäßigen Abständen** selbstständig durch die jeweiligen Nutzerinnen und Nutzern aktualisiert werden, um Datenverlust und eine Sperrung des Gerätes zu vermeiden.

> Die Aktualisierung wird nur eingeleitet, wenn eine Netzwerk-Verbindung via **LAN-Kabel** oder über **BUWVPN** besteht.

Schritt-für-Schritt-Anleitung

> Bitte erstellen Sie immer eine Datensicherung, bevor Sie Änderungen an Ihrem System vornehmen.

Folgende Schritte bringen den ZENworks-Agenten auf den neuesten Stand:

- Im Windows-System mit Ihrem **Benutzernamen anmelden** (wenn nicht schon geschehen)
- Rechner via **LAN** oder **BUWVPN** verbinden (wenn nicht schon geschehen)
- Im rechten Abschnitt der unteren **Taskleiste** auf das **blaue Symbol "ZENworks"** rechtsklicken und **"Aktualisieren"** klicken. Ein rotierender schwarz-weißer Kreis erscheint. **HINWEIS:** Bitte warten Sie so lange, bis das Symbol wieder blau eingefärbt ist
- Im Anschluss Ihren **Benutzer abmelden** und **erneut anmelden**
- Nun startet der Update-Prozess. Bitte den dortigen Anweisungen folgen

Es kann u.U. vorkommen, dass Ihr System einige Minuten für die Aktualisierung benötigt. Nach Abschluss des Update-Prozesses sollten Sie Ihr Endgerät wieder wie gewöhnlich nutzen können.

Neubereitstellung von ZDM-Geräten

Was ist eine Neubereitstellung?

Die Neubereitstellung ist ein wichtiger Prozess, bei dem ZDM-Geräte komplett gelöscht und das Betriebssystem Windows neu installiert wird. Ziel ist es, den Zustand aller zentral verwalteten Geräte konsistent zu halten, was die Fehleranfälligkeit des Systems verringert.

Erste Schritte nach der Neubereitstellung

Nachdem ein ZDM-Gerät neu bereitgestellt wurde, müssen einige wichtige Schritte durchgeführt werden, um sicherzustellen, dass Sie effektiv arbeiten können und alle notwendigen Dienste und Programme korrekt eingerichtet sind.

Vollständige Synchronisation des Nutzerprofils

- **Verbindung herstellen:** Stellen Sie sicher, dass das ZDM-Gerät per Kabel mit dem Uni-Computer-Netz verbunden ist
- **Synchronisation:** Bei der ersten Anmeldung nach der Neubereitstellung erfolgt eine vollständige Synchronisation Ihres Nutzerprofils. Dies legt Ihr Nutzerprofil erstmalig lokal an, sodass Sie in Zukunft auch auf Ihre Daten zugreifen können, wenn Sie nicht mit dem Uni-Netz verbunden sind (z.B. im Homeoffice oder auf Dienstreisen). Daher dauert die erste Anmeldung etwas länger

> Wir empfehlen dringend, regelmäßig eine solche Verbindung herzustellen. Nur so wird ein Backup Ihrer Daten angelegt und wichtige Softwareupdates eingespielt.

Erstmalige Anmeldung bei Outlook/ Office365

- **Anmeldung:**
  - Melden Sie sich mit Ihren **universitären Zugangsdaten (we\abcd1234)** in **Outlook** an
  - Anschließend werden Sie noch aufgefordert, sich bei **Office365** anzumelden. Hier verwenden Sie die **Email** und das **Passwort**, welche Sie bei der Registrierung im Softwareportal angegeben haben. Damit haben Sie Zugriff auf alle Office-Programme und Dienste
- **Einrichtung:** Folgen Sie den Anweisungen zur Einrichtung Ihres Kontos und stellen Sie sicher, dass alle notwendigen Programme korrekt installiert und aktiviert sind

> In wenigen Fällen kann es passieren, dass die Anwendung wiederholt nach dem Passwort fragt. Sie lösen dieses Problem indem Sie Ihr Outlook365 Profil zurücksetzen. Wenn Outlook nach dem Neustart geöffnet wird, fragt es einmal mehr nach dem Passwort. Setzen Sie den Haken bei "Anmeldedaten speichern". Schließen Sie Outlook nach dem Sie sich erfolgreich angemeldet haben und öffnen Sie es wieder. Es sollte nun korrekt eingerichtet sein.

Erstmalige Anmeldung bei Adobe Creative Cloud (falls verwendet)

- **Anmeldung:** Wenn Sie Adobe Creative Cloud nutzen, melden Sie sich mit den dafür vorgesehenen universitären Zugangsdaten an
- **Installation:** Wählen Sie die benötigten Programme aus und installieren Sie diese entsprechend
- Für die Einrichtung, verwenden Sie gerne die Anleitung vom SCC

Erstmalige Anmeldung bei Nextcloud (falls verwendet)

- **Anmeldung:** Für die Nutzung von Nextcloud, melden Sie sich ebenfalls mit Ihren universitären Zugangsdaten an
  - **Server-Adresse:** https://nextcloud.uni-weimar.de
- **Synchronisation:** Richten Sie gegebenenfalls die Synchronisation Ihrer Dateien ein, um einen reibungslosen Zugriff und ein effizientes Arbeiten zu gewährleisten
- Weitere Informationen finden Sie hier

Abschluss

Nachdem Sie diese Schritte durchgeführt haben, ist Ihr ZDM-Gerät vollständig eingerichtet und bereit für den Einsatz. Für weitere Unterstützung oder bei Fragen wenden Sie sich bitte an it-support@archit.uni-weimar.de.

Wir wünschen Ihnen einen guten Start und produktives Arbeiten mit Ihrem neu bereitgestellten ZDM-Gerät.

BitLocker-Recovery nach Lenovo-Firmware- oder BIOS-Update

Bei einzelnen zentral verwalteten Lenovo-Notebooks kann es nach einem Firmware- oder BIOS-Update vorkommen, dass Windows beim Start den **BitLocker-Recovery-Schlüssel** anfordert.

Kurzfassung

Wenn Ihr Gerät beim Einschalten oder Neustarten einen blauen BitLocker-Bildschirm anzeigt und nach einem Wiederherstellungsschlüssel fragt, ist das Gerät normalerweise nicht defekt. Windows benötigt in diesem Fall den passenden Wiederherstellungsschlüssel, bevor es wieder startet.

Bitte führen Sie keine Neuinstallation durch und ändern Sie keine BIOS- oder UEFI-Einstellungen.

Warum erscheint diese Abfrage?

BitLocker schützt die Daten auf dem Gerät durch Verschlüsselung. Beim Start prüft Windows, ob sich sicherheitsrelevante Start-, Firmware- oder BIOS-Einstellungen verändert haben.

Ein Firmware- oder BIOS-Update kann solche Einstellungen technisch berühren. Windows interpretiert das in einzelnen Fällen als sicherheitsrelevante Änderung und fordert deshalb den BitLocker-Recovery-Schlüssel an.

Das ist eine Schutzfunktion. Es bedeutet nicht automatisch, dass Daten verloren sind oder das Gerät neu installiert werden muss.

Was soll ich als Nutzerin oder Nutzer tun?

Erstellen Sie bitte ein Ticket an:

`it-support@archit.uni-weimar.de`

Bitten Sie darin um den BitLocker-Recovery-Schlüssel und nennen Sie, wenn möglich:

- Ihren Namen
- den Gerätenamen, falls sichtbar
- das Gerätemodell, falls bekannt
- dass eine BitLocker-Recovery-Abfrage angezeigt wird

Alternativ können Sie das Gerät zu uns bringen. ITAU kann den Fall vor Ort prüfen und den BitLocker-Recovery-Schlüssel kontrolliert eingeben.

Kontakt

Bei Fragen wenden Sie sich an den IT-Support der Fakultät Architektur und Urbanistik:

`it-support@archit.uni-weimar.de`

ZDM-Rechner für Präsentationen wach halten / automatische Bildschirmsperre

Wenn ein zentral verwalteter Windows-Rechner (ZDM) für eine Präsentation, Ausstellung oder Beamer-Daueranzeige genutzt wird, soll der Bildschirm oft über längere Zeit aktiv bleiben.

Die zentral verwalteten Sicherheitsfunktionen, wie automatische Sperrung oder Richtlinien des ZDM, können nicht dauerhaft deaktiviert werden. Für Präsentationen kann stattdessen der Windows-Präsentationsmodus verwendet werden.

Präsentationsmodus aktivieren

Gehen Sie am ZDM-Rechner wie folgt vor:

- Drücken Sie `Windows-Taste + X`
- Wählen Sie `Mobilitätscenter`
- Klicken Sie im Bereich `Präsentationseinstellungen` auf `Einschalten`

Der Präsentationsmodus ist speziell für Präsentationen vorgesehen. Er verhindert unter anderem, dass während der Präsentation automatisch der Bildschirmschoner startet, der Bildschirm abgedunkelt wird oder der Rechner den Bildschirm sperrt.

Wichtig

> Die zentral verwalteten ZDM-Sicherheitsfunktionen können nicht deaktiviert werden. Nutzen Sie für Präsentationen den Präsentationsmodus statt Änderungen an den Energie- oder Sperreinstellungen.

Nach der Präsentation

Deaktivieren Sie den Präsentationsmodus nach Ende der Präsentation wieder, damit die normalen Energie- und Sicherheitseinstellungen greifen.