Intel® Active Management Technology: गोपनीयता विवरण

आखिरी बार संशोधन: 8/12/ 2021

Intel Corporation आपकी गोपनीयता की रक्षा करने के लिए प्रतिबद्ध है. इस कथन में यह बताया गया है कि Intel® Active Management Technology (Intel® AMT) , गोपनीयता के नज़रिए से किन संवेदनशील कामों और क्षमताओं को चालू करता है और Intel AMT, IT प्रशासकों को क्या करने की अनुमति देता है और क्या नहीं करने देता. साथ ही, यह बताता है कि Intel AMT, उपयोगकर्ता के सिस्टम पर किस तरह का डेटा स्टोर करता है. यह कथन सिर्फ़ Intel के ऑनलाइन निजता नोटिस को पूरा करता है और सिर्फ़ Intel AMT पर लागू होता है.

Intel AMT क्या है?

Intel AMT, अधिकृत IT एडमिन की मदद से कंपनी में, नेटवर्क कंप्यूटर सिस्टम के आउट-ऑफ़-बैंड (OOB) में दूसरी जगह से सहायता देने और प्रबंध करने की प्रक्रिया चालू करता है.

Intel AMT के द्वारा उठाए गए गोपनीयता के संभावित मुद्दे क्या हैं?

रिमोट प्रबंधन क्षमताएँ सॉफ़्टवेयर विक्रेताओं से उपलब्ध हैं, और बहुत सी संगठनों के IT विभागों द्वारा काफी समय से उपयोग हो रही है.

हालांकि, Intel AMT, IT व्यवस्थापक को उपयोगकर्ता के कंप्यूटर पर दूसरी जगह से सहायता देने और उसे संचालन करने की अनुमति देता है. भले ही, उपयोगकर्ता मौजूद न हो या उसका कंप्यूटर बंद हो.

उपयोगकर्ता कैसे बता सकता है कि सिस्टम पर Intel AMT चालू है की नहीं?

Intel ने Intel AMT के मौजूदा स्टेटस के बारे में असली उपयोगकर्ता को पारदर्शिता और सूचना देने के लिए, एक सिस्टम ट्रे आइकॉन बनाया है. मौजूदा समय में, स्टैंडर्ड Intel AMT सॉफ़्टवेयर में एक Intel® Management and Security Status (IMSS)आवेदन और सिस्टम ट्रे आइकॉन शामिल है, जो ड्राइवर और सुविधाओं के साथ इंस्टॉल किया गया है. IMSS सिस्टम ट्रे आइकॉन, सिस्टम पर Intel AMT का मौजूदा स्टेटस (चालू या बंद) दिखाता है. साथ ही, इसमें Intel AMT को चालू/बंद करने के निर्देश भी प्रदान करता है. Intel का सुझाव है कि हर मूल उपकरण निर्माता (OEM) IMSS ऐप्लिकेशन को लोड करे. हालांकि, OEM के पास यह फ़ैसला करने का अधिकार है कि वे Intel का सुझाव माने या नहीं. इसके अलावा, असली उपयोगकर्ता का IT प्रबंधक, असली उपयोगकर्ताओं को Intel AMT की सुविधा वाला सिस्टम देने से पहले IMSS ऐप्लिकेशन को हटा सकते हैं. OEM जो सुविधा चुनते हैं, उसके आधार पर, उपयोगकर्ता भी अपने कंप्यूटर के सिस्टम BIOS में Intel AMT का स्टेटस देख सकते हैं. हालांकि, यह ध्यान रखना ज़रूरी है कि हो सकता है कुछ कंपनियों के IT विभाग, उपयोगकर्ताओं को सिस्टम BIOS को

ऐक्सेस करने के लिए इस्तेमाल की जाने वाली ज़रूरी प्रक्रिया का एक्सेस ना दे, जिससे Intel AMT चालू/बंद होता है या Intel AMT का स्टेटस पता चलता है.

Intel AMT, उपयोगकर्ता से कौनसी निजी जानकारी लेता है?

Intel AMT, उपयोगकर्ता से कोई भी निजी जानकारी (उदाहरण के लिए, नाम, पता, फ़ोन नंबर वगैरह) नहीं लेता है.

Intel AMT द्वारा Intel Corporation को किस प्रकार की जानकारी भेजी जाती है और उस जानकारी का उपयोग कैसे किया जाता है?

Intel AMT कोई डेटा नहीं भेजता है Intel Corporation को.

Intel AMT किस तरह की जानकारी संग्रहीत करता है?

Intel AMT, सिस्टम के मदरबोर्ड पर फ़्लैश मेमोरी में जानकारी संग्रहीत करता है. इस जानकारी में फ़र्मवेयर कोड, हार्डवेयर इन्वेंट्री डेटा (उदाहरण के लिए, मेमोरी का साइज़, CPU का प्रकार, हार्ड-डिस्क का प्रकार), एक इवेंट लॉग जो प्लेटफ़ॉर्म इवेंट रिकॉर्ड करता है (उदाहरण के लिए, CPU का गर्म होना, पंखा खराब होना, BIOS POST सन्देश), Intel AMT के सुरक्षा इवेंट शामिल है (उदाहरण के लिए, Intel AMT के पासवर्ड में गड़बड़ी होने का इवेंट या सिस्टम डिफेंस फ़िल्टर ट्रिपिंग की चेतावनी). साथ ही, Intel AMT कॉन्फ़िगरेशन डेटा (उदाहरण के लिए, नेटवर्क सेटिंग, ऐक्सेस कंट्रोल की सूचियां, और यूनिवर्सल यूनिक आइडेंटिफ़ायर (UUIDs), जिसमें प्रावधान डेटा, LAN MAC का पता, कुंजियां, कीबोर्ड-वीडियो-माउस (KVM) के पासवर्ड, ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) सर्टिफ़िकेट और IT की तरफ़ से कॉन्फ़िगर की गई वायरलेस नेटवर्क प्रोफ़ाइल भी शामिल हैं) शामिल है. संवेदनशील समझे जाने वाले सभी कॉन्फ़िगरेशन डेटा को, फ़्लैश पर एन्क्रिप्टेड रूप में संग्रहीत किया जाता है. UUID से जुड़ी ज़्यादा जानकारी के लिए, नीचे दिया गया अनुभाग देखें.

Intel AMT का 11.0 और पुराना वर्ज़न, रजिस्टर किए गए स्वतंत्र सॉफ़्टवेयर विक्रेता (ISV) ऐप्लिकेशन को, फ़्लैश मेमोरी रिपॉज़िटरी के एक हिस्से में डेटा संग्रहीत करने की अनुमति देता है, जिसे तीसरे-पक्ष के डेटा स्टोर के रूप में जाना जाता है (3PDS). Intel AMT संस्करण 11.6 में शुरू करते हुए, इस विशेषता को वेब एप्लिकेशन होस्टिंग से बदल दिया गया था जो Intel AMT को नष्ट न होने वाली मेमोरी (NVM) में वेब एप्लिकेशन को होस्ट करने की सुविधा देता है जिसे Intel AMT ग्राहक मंच पर स्थानीय रूप से प्रबंधित करता है.

Intel अपने ISV को ज़िम्मेदारी से डेटा मैनेज करने के लिए गोपनीयता सुविधाओं से जुड़े सबसे अच्छे तरीके बताता है. इसलिए, Intel यह तय नहीं करता है कि फ़्लैश मेमोरी के इस हिस्से में कौन सा डेटा स्टोर किया जा सकता है और ISV डेटा के लिए एन्क्रिप्शन के तरीकों का समर्थन नहीं करता. इसलिए, ISV को सुझाव दिया जाता है कि अगर वे अपने डेटा को संवेदनशील मानते हैं तो इसे फ़्लैश मेमोरी पर संग्रहीत करने से पहले अपने डेटा को एन्क्रिप्ट कर लें. अगर आपको यहां स्टोर किए गए डेटा की वजह से गोपनीयता से जुड़े जोखिमों का डर है, तो कृपया NVM में स्टोर की गई जानकारी और वेब ऐप्लिकेशन के

प्रकार के बारे में और ज़्यादा जानने और और इसकी सुरक्षा कैसे की जाती है यह जानने के लिए, इससे जुड़े तीसरे-पक्ष के सॉफ़्टवेयर डेवलपर से संपर्क करें.

Intel AMT, UUID का इस्तेमाल कैसे करता है? Intel AMT की सुविधा वाले प्लेटफ़ॉर्म पर UUID कौनसी सुविधाएं चालू करता है और कौनसी सुविधाएं नहीं?

यूनिवर्सल यूनिक आइडेंटिफ़ायर (UUID), Intel AMT के कई कामों के लिए इस्तेमाल किए जाने वाले आर्टिफ़ैक्ट हैं, जिनमें प्रावधान की प्रक्रिया, सिस्टम की सुरक्षा (उदाहरण के लिए, पासवर्ड, कुंजियां और TLS प्रमाणपत्र) शामिल हैं. साथ ही, इन्हें यह पक्का करने के लिए भी इस्तेमाल किया जाता है कि IT एडमिन किसी कंपनी के अंदर किसी उपयोगकर्ता के सिस्टम से सही तरीके से कनेक्ट हो पाएं और मैनेज कर पाएं.

Intel VPRO प्लेटफ़ॉर्म, स्थायी UUID के साथ आता है जिसे Intel® Unique Platform ID (UPID) कहा जाता है. ऐसा इसलिए, ताकि इससे उन कामों को चालू किया जा सके जिनके लिए स्थायी UUID की ज़रूरत होती है, जैसे कि ज़ीरो-टच का प्रावधान. UPID की कार्यक्षमता, OEM कार्यान्वयन पर निर्भर है. UUID लगभग सभी आधुनिक कंप्यूटर में मौजूद हैं और आमतौर पर, OEM इन्हें सभी प्लेटफ़ार्म पर इंस्टॉल करते हैं. इसमें Intel AMT का कोई हाथ नहीं होता. दरअसल, मौजूदा समय में UUID को कई कंप्यूटर पर पाए जाने वाले ऐप्लिकेशन में इस्तेमाल किया जाता है, ताकि ज़रूरी काम पूरे करने के लिए सिस्टम की यूनीक जानकारी को अलग किया जा सके, जैसे कि OS की डिलीवरी या वायरस नियंत्रण करने वाले सिस्टम को अपडेट करना. Intel AMT, UUID का इस्तेमाल बहुत समान तरीके से करता है – पहला अंतर यह है कि Intel AMT को UUID OOB तक पहुंचने के लिए चालू करने के लिए, UUID को फ़्लैश मेमोरी रिपॉज़िटरी में कॉपी किया जाता है.

यह ध्यान रखना ज़रूरी है कि Intel AMT की सुविधा वाले सिस्टम पर, Intel अपने उपयोगकर्ताओं या उनके कंप्यूटर को ट्रैक करने के लिए UUID का इस्तेमाल नहीं कर सकता, न ही वे Intel को प्लेटफ़ॉर्म के छिपे हुए तरीके से उपयोगकर्ता का सिस्टम ऐक्सेस करने की अनुमति देता है और न ही वे Intel को उपयोगकर्ता की सहमति के बिना फ़र्मवेयर को प्लेटफ़ॉर्म पर ज़बरदस्ती इंस्टॉल करने की अनुमति देता है. यह सभी नियम UPID पर भी लागू होते हैं. Intel AMT ने फ़्लैश मेमोरी में जो भी UUID स्टोर किया है उसे सिर्फ़, Intel AMT की सुविधा वाले किसी प्लेटफ़ॉर्म के लिए पुष्टि किया गया IT एडमिन ही ऐक्सेस कर सकता है. पुष्टि किए गए IT एडमिन की सूची को असली उपयोगकर्ता IT ने एंटरप्राइज़ सर्टिफ़िकेट या Intel AMT सिस्टम पर शारीरिक तौर पर उपस्थित होने की प्रक्रिया (BIOS मेन्यू या USB कुंजी के ज़रिए) का इस्तेमाल करके एक सुरक्षित प्रक्रिया के दौरान कॉन्फ़िगर किया है, ताकि भरोसा बनाया जा सके. इसलिए, यह असली उपयोगकर्ता IT के बताए गए भरोसेमंद सर्वर पर रहने वाले कंसोल के साथ दिखता है. दूसरे शब्दों में कहें, तो Intel AMT के ज़रिए न तो UUID और न ही किसी अन्य जानकारी को किसी बाहरी पक्ष से लेकर किसी असली उपयोगकर्ता तक पहुंचाया या लिया नहीं जा सकता, जब तक कि असली उपयोगकर्ता इसे साफ़ तौर पर कॉन्फ़िगर नहीं करता. किसी सिस्टम के लिए पुष्टि किए गए एडमिन की पहचान करने के लिए https://software.intel.com/en-us/business-client/manageability पर उपलब्ध Intel AMT सॉफ़्टवेयर डेवलपर किट (SDK) के दस्तावेज़ देखें, जो ACL या केर्बरोस के पुष्टि किए गए अकाउंट को फिर से पाने के लिए एक API देता है.

Intel® Active Management Technology (Intel® AMT), सभी नेटवर्क पर किस तरह की जानकारी भेजता है?

Intel AMT, पहले से तय किए गए IANA नेटवर्क पोर्ट पर डेटा भेजता और लेता है: SOAP/HTTP के लिए पोर्ट 16992, SOAP/HTTPS के लिए पोर्ट 16993, रीडायरेक्शन/TCP के लिए पोर्ट 16994 और रीडायरेक्शन/TLS के लिए पोर्ट 16995. DASH का पालन करने वाले सिस्टम, HTTP के लिए पोर्ट 623 और HTTPS के लिए 664 पर डेटा भेजेंगे और लेंगे. कीबोर्ड-वीडियो-माउस (KVM) सेशन ऊपर बताए गए रीडायरेक्शन पोर्ट (16994 या 16995) पर या पारंपरिक RFB (VNC सर्वर) पोर्ट - 5900 पर चल सकता है. नेटवर्क पर जिस तरह की जानकारी भेजी जाएगी उसमें Intel AMT कमांड और प्रतिक्रिया संदेश, पुनर्निर्देशन ट्रैफ़िक और सिस्टम चेतावनी शामिल हैं. अगर उपयोगकर्ता के सिस्टम पर यह विकल्प चालू होता है, तो पोर्ट 16993 और 16995 पर प्रसारित किया गया डेटा, ट्रांसपोर्ट-लेयर सिक्योरिटी (TLS) से सुरक्षित रहता है.

Intel AMT, IPV4 या IPV6 नेटवर्क पर डेटा भेज सकता है और RFC 3041 गोपनीयता एक्सटेंशन के मुताबिक काम करता है.

Intel® Active Management Technology (Intel® AMT) नेटवर्क पर, पहचानी जा सकने वाली कौनसी जानकारी दिखाई जाती है?

अगर Intel® AMT चालू है, तो खुले हुए पोर्ट ऐसी जानकारी दिखाएंगे जिसका उपयोग नेटवर्क पर अन्य लोगों को कंप्यूटर की पहचान करने के लिए किया जा सकता है. इसमें HTTPS प्रमाणपत्र, HTTP रखने की जगह, Intel AMT संस्करण और अन्य जानकारी शामिल है, जिसका इस्तेमाल कंप्यूटर को पहचानने के लिए किया जा सकता है. यह सुचना Intel® AMT द्वारा समर्थित प्रोटोकॉल के सामान्य संचालन के भाग के रूप में दी गई है. कोई ऑपरेटिंग सिस्टम फ़ायरवॉल, Intel® AMT पोर्ट का ऐक्सेस नहीं रोक सकता. हालांकिं, एडमिन Intel® AMT के स्थानीय पोर्ट को बंद करने और इस जानकारी के ऐक्सेस को सीमित करने के लिए, जगह का पता लगाने और मदद के लिए फ़ास्ट कॉल (CIRA) का इस्तेमाल कर सकता है.

Intel AMT, पुष्टि किए गए किसी IT प्रशासक को किन कामों की अनुमति देता है?

- दूसरी जगह से डिवाइस चालू करना, बंद करना और और समस्या ठीक करने और मरम्मत के लिए सिस्टम को रीबूट करना.
- होस्ट OS के बंद या खराब होने पर भी, दूसरी जगह से सिस्टम को ठीक करना.
- दूसरी जगह से, सिस्टम पर BIOS कॉन्फ़िगरेशन सेटिंग देखना और बदलना. Intel AMT में विकल्प है कि IT प्रशासक, BIOS पासवर्ड की प्रक्रिया से बचकर निकल सकते हैं, लेकिन सभी OEM इस सुविधा को लागू नहीं करते.
- प्रणाली की सुरक्षा के लिए नेटवर्क ट्रैफ़िक फ़िल्टर को कॉन्फ़िगर करें.

- सिस्टम पर डाले गए ऐप्लिकेशन की निगरानी करें (उदाहरण के लिए, क्या एंटीवायरस सॉफ़्टवेयर चल रहा है).
- उपयोगकर्ता के सिस्टम पर, Intel AMT फ़र्मवेयर रिपोर्टिंग की तरफ़ से जनरेट किए गए वे चेतावनी पाएं जिनके लिए तकनीकी सहायता की ज़रूरत हो सकती है. जैसे: CPU का गर्म होना, पंखा खराब होना या सिस्टम डिफेंस फ़िल्टर ट्रिपिंग. इसके अलावा, सार्वजनिक तौर पर और उदाहरण www.intel.com/software/manageability पर दिए गए हैं.
- बूट प्रक्रिया को फ़्लॉपी डिस्क, CD-ROM या IT एडमिन के सिस्टम पर मौजूद एक इमेज पर रीडायरेक्ट करके, उपयोगकर्ता के सिस्टम को दूसरी जगह से ठीक करें.
- उपयोगकर्ता के सिस्टम पर कीबोर्ड इनपुट और टेक्स्ट-मोड वीडियो आउटपुट को, IT एडमिन के सिस्टम पर रीडायरेक्ट करके सिस्टम को दूसरी जगह से ठीक करें.
- उपयोगकर्ता के सिस्टम से और IT एडमिन के सिस्टम (KVM रीडायरेक्शन) पर कीबोर्ड, वीडियो और माउस को रीडायरेक्ट करके सिस्टम को दूसरी जगह से ठीक करें.
- कॉन्फ़िगर करें कि किस नेटवर्क की जगह में, Intel AMT की मैनेज करने की सुविधा ऐक्सेस की जा सकेगी (उदाहरण के लिए, भरोसेमंद डोमेन की जानकारी देकर).
- फ़्लैश रिपॉज़िटरी (यानी की 3PDS एरिया) पर डेटा लिखने/हटाने के लिए एक रजिस्टर किए गए ISV ऐप्लिकेशन का इस्तेमाल करें
- नष्ट ना होने वाली मेमोरी में (NVM) वे वेब ऐप्लिकेशन होस्ट करें जिन्हें Intel AMT, ग्राहक प्लेटफ़ॉर्म (Intel AMT 11.6 और नए वर्ज़न) पर स्थानीय रूप से मैनेज करता है.
- UUID के ज़रिए, कंपनी के नेटवर्क पर उपयोगकर्ता के प्रणाली की पहचान करें.
- Intel AMT का प्रावधान रद्द करें और फ़्लैश कंटेंट हटाएं.
- प्री-कॉन्फ़िगर्ड क्लाइंट-इनिशिएटेड-रिमोट-ऐक्सेस (CIRA) प्रोफ़ाइल का इस्तेमाल करके, कंपनी के नेटवर्क के बाहर भी दूसरी जगह से सिस्टम को जोडा जा सकता है.

क्या Intel AMT, पुष्टि किए गए किसी IT प्रशासक को उपयोगकर्ता की स्थानीय हार्ड ड्राइव तक पहुंचने की अनुमति देता है?

दूसरी जगह से किए जा रहे प्रबंधन सत्र के दौरान, IT प्रशासक के पास उपयोगकर्ता के स्थानीय हार्ड ड्राइव तक पहुंचने का एक्सेस होता है. इसका मतलब यह है कि IT प्रशासक, उपयोगकर्ता की हार्ड डिस्क से फ़ाइलें पढ़/लिख सकता है. उदाहरण के लिए, गड़बड़ी वाले किसी ऐप्लिकेशन या ओएस को ठीक करके या फिर से इंस्टॉल करके उपयोगकर्ता का सिस्टम ठीक करना. Intel AMT दो सुविधाएं इस्तेमाल करता है, जो उन संभावित गोपनीयता जोखिमों को कम करने में सहायता करता है जो IT एडमिन को इस तरह की जानकारी का ऐक्सेस देने से हो सकते हैं: IMSS और ऑडिट लॉगिंग. ऑडिट लॉगिंग सुविधाएं, Intel AMT के ज़रिए, उपयोगकर्ता सिस्टम में IT एडमिन के ऐक्सेस की सूची लॉग करके, एडमिन की जवाबदेही के लिए एक रास्ता बनाती हैं. हालांकि, असल में कौनसे इवेंट लॉग किए जाएंगे यह ऑडिटर बताता है, जो आमतौर पर कंपनी में उपयोगकर्ता नहीं होता. Intel अपने ग्राहकों को सलाह देता है कि Intel AMT सिस्टम को दूसरी जगह से ऐक्सेस करना उस तरह की जानकारी है जिसे लॉग किया जाना चाहिए, पर यह संभव है कि कुछ कंपनियों में यह जानकारी उपयोगकर्ताओं के लिए उपलब्ध न हो. IMSS, उपयोगकर्ताओं

को उन मौकों की सूचना कैसे दे सकता है जब IT एडमिन उनके सिस्टम को ऐक्सेस करते हैं, इसके बारे में नीचे जानकारी दी गई है.

क्या Intel AMT KVM रीडायरेक्शन, पुष्टि किए गए किसी IT एडमिन को उपयोगकर्ता का कंप्यूटर, दूसरी जगह से इस तरह कंट्रोल करने की अनुमति देता है जैसे कि वह खुद ही अपने कीबोर्ड पर बैठे हों?

KVM रीडायरेक्शन से दूसरी जगह से किए जा रहे मैनेजमेंट सेशन के दौरान, IT एडमिन के पास उपयोगकर्ता के कंप्यूटर पर वैसा ही कंट्रोल होता है जैसे कि वह अपने कंप्यूटर पर बैठे हों. KVM रीडायरेक्शन सेशन के लिए, Intel AMT यह शर्त लागू करता है कि KVM सेशन को उपयोगकर्ता की साफ़ सहमति के बिना शुरू नहीं किया जा सकता है, जिसे KVM उपयोगकर्ता सहमति के रूप में जाना जाता है. रीडायरेक्शन सेशन में पूरी तरह से उपयोगकर्ता की सहमति लागू करने के लिए, किसी भी अन्य विंडो के ऊपर, उपयोगकर्ता की स्क्रीन पर एक सुरक्षित आउटपुट विंडो ("स्प्राइट") दिखाई जाती है, जिसमें उपयोगकर्ता को IT एडमिन के सामने, अनियमित तौर पर बना हुआ कोई नंबर पढ़कर सुनाना होता है. अगर IT प्रशासक सही सत्र नंबर डालता है, तो ही KVM सेशन शुरू होगा. वैध KVM सेशन शुरू होने के बाद, उपयोगकर्ता की पूरी स्क्रीन पर लाल और पीले रंग का चमकदार बॉर्डर आ जाएगा – जो यह दिखाता है कि IT एडमिन KVM को ठीक करने का सेशन कर रहे हैं. सत्र के चालू रहने तक, लाल और पीले रंग का यह बॉर्डर दिखता रहेगा. ध्यान दें कि जब Intel AMT सिस्टम, ग्राहक नियंत्रण मोड में होता है तो KVM उपयोगकर्ता की सहमति ज़रूरी होती है, लेकिन प्रशासक नियंत्रण मोड में यह विकल्प के तौर पर होती है.

OEM की सेटिंग्स के अनुसार, Intel AMT में SOL/IDER या KVM सुविधाएं, Intel® Management Engine BIOS Extension (Intel® MEBX) में चालू या बंद की जाती हैं. IT प्रशासक, KVM की सहमति देने वाली शर्तों को BIOS सेटिंग या Intel AMT कॉन्फ़िगरेशन सेटिंग के ज़रिए बदल सकते हैं. Intel का सुझाव है कि उपयोगकर्ता की गोपनीयता बनाए रखने के लिए, उसकी सहमति की शर्त का इस्तेमाल किया जाए.

उपयोगकर्ता को कैसे पता चलेगा कि किसी IT प्रशासक ने Intel AMT के ज़रिए सिस्टम ऐक्सेस किया है या नहीं?

IMSS सिस्टम ट्रे आइकॉन कई इवेंट के लिए उपयोगकर्ता की सूचना को चालू करता है और मदद करता है. इसमें यह सूचना शामिल है कि कोई IT प्रशासक दूसरी जगह से चलने वाले रीडायरेक्शन सेशन (यानी कि SOL/IDER) को खोलने/बंद करने के ज़रिए, उपयोगकर्ता का सिस्टम ऐक्सेस कर रहा है या किया था. साथ ही, सिस्टम डिफ़ेंस एक्टिविशेन और IT प्रशासक की तरफ़ से उपयोगकर्ता के सिस्टम को दूसरी जगह से ठीक करना भी शामिल है. इसके अलावा, दूसरी जगह से किए जाने वाले पुनर्निर्देशन सत्र के दौरान, स्क्रीन के ऊपरी दाएं कोने में एक चमकता हुआ आइकॉन दिखेगा. हालांकि, असल में जो इवेंट IMSS की तरफ़ से एंटरप्राइज़ सेटिंग में चालू किए जाते हैं, उन्हें IT प्रशासक बताता है, उपयोगकर्ता नहीं. जबकि Intel अनुशंसा करता है कि Intel AMT सिस्टम तैनात करने वाले उद्यम इस पैराग्राफ में

उल्लिखित IMSS अधिसूचनाओं को सक्षम करें, यह संभव है कि Intel AMT सिस्टम के दूरस्थ कनेक्शन के बारे में जानकारी सभी उपयोगकर्ताओं के लिए उपलब्ध नहीं हो सकती है.

कोई उपयोगकर्ता सभी Intel AMT कॉन्फ़िगरेशन और निजी डेटा को कैसे साफ़ कर सकता है?

Intel AMT BIOS विकल्प प्रदान करता है ताकि एक Intel AMT सिस्टम को आंशिक/पूरी रूप से अप्राब्द किया जा सके. Intel, असली उपयोगकर्ताओं को सुझाव देता है कि पुनर्विक्रय/पुनर्चक्रण करने से पहले, सिस्टम से हर प्रावधान हटा दें और अगर आप Intel AMT की सुविधा वाला सिस्टम खरीदते हैं, तो पुष्टि करें कि Intel AMT के प्रावधान को पूरी तरह से हटा दिया गया है.

निजता कथन अपडेट

हम कभी-कभी इस निजता कथन को अपडेट कर सकते हैं. जब हम ऐसा करेंगे, तो हम निजता कथन के सबसे ऊपर, आखिरी बार अपडेट किए जाने की तारीख बदल देंगे.

ज़्यादा जानकारी के लिए

अगर आपके कोई सवाल हैं या आप इस गोपनीयता पूरक के बारे में ज़्यादा जानना चाहते हैं, तो हमसे यह फ़ॉर्म संपर्क करने के लिए कृपया का इस्तेमाल करें.

गोपनीयता सूचना लिंक

- Intel गोपनीय सूचना
- उम्मीदवार के लिए नोटिस